comnet
Communication Networks

INSTALLATION AND OPERATION MANUAL

CWGE9MS

COMMERCIAL GRADE 9 PORT GIGABIT MANAGED ETHERNET SWITCH WITH (7) 10/100/1000TX + (2) 1000FX SFP OR 10/100/1000TX PORTS

V1.02 – October 2010

The ComNet™ CWGE9MS Managed Ethernet Switch provides transmission of (7) 10/100/1000 BASE-TX and (2) 1000FXcombo ports. These units are available for use with either conventional CAT-5e copper or optical transmission media. Ports 1 – 7 support the 10/100/1000 Mbps Ethernet IEEE 802.3 protocol, and auto-negotiating and auto-MDI/MDIX features are provided for simplicity and ease of installation. Ports 8 – 9 are 10/100/1000 configurable for copper or 1000 fiber media for use with multimode or single mode optical fiber without need for configuration, selected by optional SFP modules. These network managed layer 2 switches are optically and electrically compatible with any IEEE 802.3 compliant Ethernet devices.

Plug-and-play design ensures ease of installation, and no electrical or optical adjustments are ever required. The CWGE9MS incorporates LED indicators for monitoring the operating status of the managed switch and network.

FCC Warning

This Equipment has been tested and found to comply with the limits for a Class-A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CE Mark Warning

This is a Class-A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Content

Chapter 1 Introduction.....6
1.1 Hardware Features 6
1.2 Software Feature.....8
1.3 Package Contents.....10
Chapter 2 Hardware Description 11
2.1 Physical Dimension.....11
2.2 Front Panel.....11
2.3 Rear Panel 12
2.4 LED Indicators.....13
Chapter 3 Hardware Installation 14
3.1 Desktop Installation.....14
3.2 Attaching Rubber Feet 14
3.3 Power On 14
Chapter 4 Network Application.....15
4.1 Desktop Application 15
4.2 Segment Application 15
4.3 X-Ring Application.....16
4.4 Coupling Ring Application 18
4.5 Dual Homing Application.....18
Chapter 5 Console Management 20
5.1 Connecting to the Console Port 20
5.2 Login in the Console Interface 20
5.3 CLI Management.....22
Chapter 6 Web-Based Management.....24
6.1 About Web-based Management 24
6.2 Preparing for Web Management.....24
6.3 System Login 25
6.4 System Information 26
6.5 IP Configuration 26
6.6 DHCP Server 27
6.6.1 System configuration 28

6.6.2 Client Entries 29
6.6.3 Port and IP Bindings 29
6.7 TFTP 30
6.7.1 Update Firmware 30
6.7.2 Restore Configuration 30
6.7.3 Backup Configuration 31
6.8 System Event Log 32
6.8.1 Syslog Configuration 32
6.8.2 SMTP Configuration 33
6.8.3 Event Configuration 35
6.9 SNTP Configuration 37
6.10 IP Security 39
6.11 User Authentication 41
6.12 Port Statistics 42
6.13 Port Control 43
6.14 Port Trunk 44
6.14.1 Aggregator setting 45
6.14.2 Aggregator Information 47
6.14.3 State Activity 48
6.15 Port Mirroring 50
6.16 Rate Limiting 51
6.17 VLAN configuration 52
6.17.1 Port-based VLAN 52
6.17.2 802.1Q VLAN 56
6.18 Rapid Spanning Tree 60
6.18.1 RSTP - System Configuration 60
6.18.2 RSTP - Port Configuration 61
6.19 SNMP Configuration 63
6.19.1 System Configuration 63
6.19.2 Trap Configuration 64
6.19.3 SNMPV3 Configuration 65

6.20 QoS Configuration 69
6.20.1 QoS Policy and Priority Type 69
6.20.2 Port-based Priority 70
6.20.3 COS Configuration 70
6.20.3 TOS Configuration 71
6.21 IGMP Configuration 72
6.22 X-Ring 73
6.23 LLDP 76
6.25.4 Multicast Filtering 77
6.23 Security-802.1X/Radius Configuration 78
6.23.1 System Configuration 78
6.23.2 Port Configuration 79
6.23.3 Misc Configuration 80
6.24 MAC Address Table 81
6.24.1 Static MAC Address 81
6.24.2 MAC Filtering 82
6.24.3 All MAC Addresses 83
6.25 Factory Default 84
6.26 Save Configuration 84
6.27 System Reboot 85
Problem Solving 86
Appendix A Command Sets 88
Commands Set List 88
System Commands Set 88
Port Commands Set 91
Trunk Commands Set 94
VLAN Commands Set 95
Spanning Tree Commands Set 98
QOS Commands Set 101
IGMP Commands Set 102
Mac / Filter Table Commands Set 103
SNMP Commands Set 104

Port Mirroring Commands Set..... 107
802.1x Commands Set..... 108
TFTP Commands Set 111
SystemLog, SMTP and Event Commands Set 111
SNTP Commands Set..... 114
X-ring Commands Set..... 116

Chapter 1 Introduction

The CWGE9MS managed Ethernet switch is a multi-port switch that can be used to build high-performance switched workgroup networks. It provides wire-speed, Fast Ethernet switching function that allows for a high-performance, low-cost connection. The switch features a store-and-forward switching and it can auto-learn and store source address on an 8K-entry MAC address table.

The CWGE9MS managed Ethernet switch has 7 auto-sensing 10/100/1000Base-TX RJ45 ports and 2 SFP/Giga copper combo port for higher connection speed.

1.1 Hardware Features

Standards	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3z Gigabit fiber IEEE 802.3ab 1000Base-T IEEE 802.3x Flow Control and Back Pressure IEEE 802.3ad Port Trunk with LACP IEEE 802.1d Spanning Tree Protocol IEEE 802.1w Rapid Spanning Tree IEEE 802.1p Class of Service IEEE 802.1q VLAN Tagging IEEE 802.1x User Authentication
Protocol	CSMA/CD
LED Indicators	Per unit: Power (Green) Per port: Link/Activity (Green), speed 1000(Green) SFP: Link/Activity (Green)

Connector	10/100/1000TX: 7 x RJ45 with Auto MDI/MDI-X function Gigabit fiber: 2 x Mini-GBIC socket Console port: RS-232 connector
Switch architecture	Store and forward switch architecture. 18Gbps system backplane. System throughput up to 26.7Mpps.
Packet buffer	1Mbits for packet buffer
RS-232 connector	One RS-232 DB-9 Female connector for switch management
Dimensions	217mm(W) x 140mm(D) x 43mm(H)
MAC Address	8K MAC address table with Auto learning function
Storage Temp.	-40℃~70℃, 95% RH
Operational Temp.	0℃~60℃, 5%~95%RH
Operational Humidity	10% to 90% (Non-condensing)
Power Supply	AC 100~240V, 50/60Hz
Power Consumption	19.3 Watts
Ventilation	1
EMI	FCC Class A, CE
Safety	UL, cUL, CE/EN60950-1

1.2 Software Feature

Management	SNMP v1 v2c, v3/ Web/Telnet/CLI Management
VLAN	Port Based VLAN IEEE 802.1Q Tag VLAN (256 entries)/ VLAN ID (Up to 4K, VLAN ID can be assigned from 1 to 4094.) GVRP (256 Groups)
Port Trunk with LACP	LACP Port Trunk: 4 Trunk groups/Maximum 4 trunk members
Spanning Tree	IEEE802.1d Spanning tree IEEE802.1w Rapid spanning tree
X-ring	Support X-ring, Dual Homing and Couple Ring Provide redundant backup feature and the recovery time below 300ms
Quality of service	The quality of service determined by port, Tag and IPv4 Type of Service, IPv4/IPv6 Different Service
Class of Service	Support IEEE 802.1p Class of Service, per port provides 4 priority queues
Port Security	Supports 100 entries of MAC address for static MAC and another 100 for MAC filter
Port Mirror	Supports 3 mirroring types: “RX, TX and Both packet”

IGMP	Support IGMP snooping v1,v2 256 multicast groups and IGMP query
IP Security	Provide 10 IP addresses that have permission to access the switch management and to prevent unauthorized intruder
Login Security	Support IEEE802.1x User-Authentication and can report to RADIUS server. ■ Reject ■ Accept ■ Authorize ■ Disable
Bandwidth Control	The egress rate control supports all of packet type and the limit rates are 100K~250Mbps Ingress filter packet type combination rules are Broadcast/Multicast/Unknown Unicast packet, Broadcast/Multicast packet, Broadcast packet only and all of packet. The packet filter rate can be set from 100k to 250Mbps
Flow Control	Support Flow Control for Full-duplex and Back Pressure for Half-duplex
System Log	Support system log record and remote system log server
SMTP	Support SMTP Server and 6 email account for receiving event alert
SNMP Trap	Up to 3 trap stations Cold start, Port link up, Port link down, Authentication failure, Private Trap for power status, X-ring topology change

SNMP MIB	RFC 1215 Trap, RFC1213 MIBII, RFC 1157 SNMP MIB, RFC 1493 Bridge MIB, RFC 2674 VLAN MIB, RFC 1643 , RFC 1757, RSTP MIB, Private MIB
DHCP	DHCP Client, DHCP Server
DNS	Provides DNS client feature and support Primary and Secondary DNS server
SNTP	Support Simple Network Time Protocol to synchronize system clock in Internet
Firmware Upgrade	Support TFTP firmware upgradeable, TFTP backup and restore
Configuration upload and download	Support text format configuration file for system quick installation

1.3 Package Contents

Unpack the contents of the CWGE9MS managed Ethernet switch and verify them against the checklist below.

- CWGE9MS managed Ethernet switch
- Power Cord
- Four Rubber Feet
- RS-232 cable
- User Manual

Compare the contents of the CWGE9MS managed Ethernet switch package with the standard checklist above. If any item is missing or damaged, please contact ComNet for service.

Chapter 2 Hardware Description

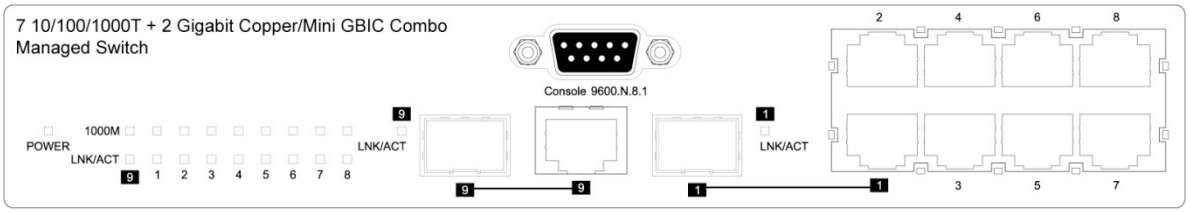
This section describes the hardware of the CWGE9MS managed Ethernet switch.

2.1 Physical Dimension

The physical dimensions of the CWGE9MS managed Ethernet switch is 217mm(W) x 140mm(D) x 43mm(H)

2.2 Front Panel

The front panel of the CWGE9MS managed Ethernet switch consists of 7x auto-sensing 10/100/1000Mbps Ethernet RJ45 ports (automatic MDI/MDIX), 2 SFP/Giga copper combo ports, and the LED indicators are also located on the front panel of the switch.



Front Panel of the 7 10/100/1000TX + 2 10/100/1000T and 1000 SFP Combo Managed Switch

RJ45 Ports (Auto MDI/MDIX)

There are 7 10/100/1000 auto-sensing RJ45 ports for 10Base-T, 100Base-TX, or 1000Base-T connections. In general, MDI means connecting to another Hub or Switch while MDIX means connecting to a workstation or PC. Therefore, Auto MDI/MDIX means that you can connect to another Switch or workstation without changing non-crossover or crossover cabling.

2 SFP/Giga copper combo port

Traditional RJ45 ports can be used for unlinking wide-band paths in short distance (<100m), or the appropriate replaceable mini-GBIC ports can be used for the application of wideband unlinking and long distance transmissions to fit the flexible field request.

2.3 Rear Panel

The 3-pronged power plug are located at the rear panel of the CWGE9MS managed Ethernet switch as shown in figure. The switch will work with AC in the range 100-240V AC, 50-60Hz.

Rear panel of the CWGE9MS managed Ethernet switch

2.4 LED Indicators

The following table provides descriptions of the LED statuses and meaning. They provide a real-time indication of systematic operation status.

LED	Status	Description
Power	Green	Power On
1000M	Yellow	The port is operating at the speed of 1000Mbps.
	Amber	The port is operating at the speed of 100Mbps.
	Off	The port is operating at the speed of 10Mbps or no device attached
LNK / ACT	Green	The port is successfully connecting with the device.
	Blinks	The port is receiving or transmitting data.
	Off	No device attached.
LNK / ACT (SFP)	Green	The port is successfully connecting with the device.
	Blinks	The port is receiving or transmitting data.
	Off	No device attached.

Chapter 3 Hardware Installation

3.1 Desktop Installation

Set the switch on a sufficiently large flat space with a power outlet nearby. The surface where you put your Switch should be clean, smooth, level, and sturdy. Make sure there is enough clearance around the Switch to allow attachment of cables, power cord and air circulation.

3.2 Attaching Rubber Feet

1. Make sure mounting surface on the bottom of the switch is grease and dust free.
2. Remove adhesive backing from your rubber feet.
3. Apply the rubber feet to each corner on the bottom of the switch. These footpads can prevent the switch from shock/vibration.

3.3 Power On

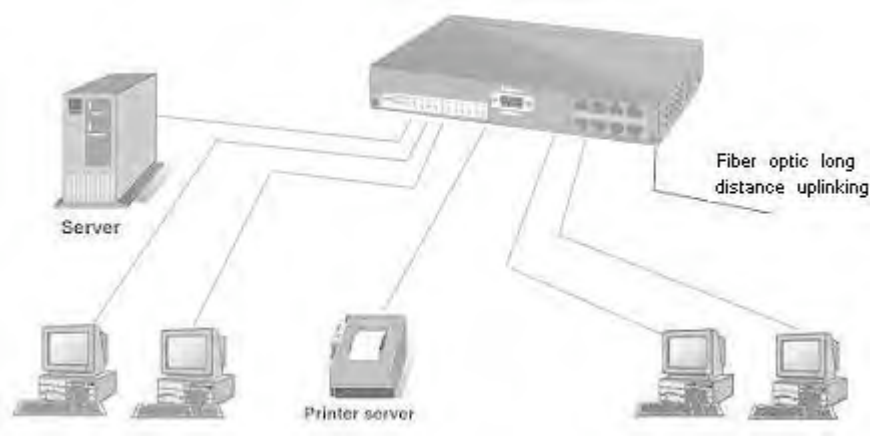
Connect the power cord to the power socket on the rear panel of the Switch. The other side of power cord connects to the power outlet. The internal power works with AC in the voltage range 90-240VAC, frequency 50~60Hz. Check the power indicator on the front panel to see if power is properly supplied.

Chapter 4 Network Application

This section provides you a few samples of network topology in which the switch is used. In general, the CWGE9MS managed Ethernet switch is designed to be used as a desktop or segment switch.

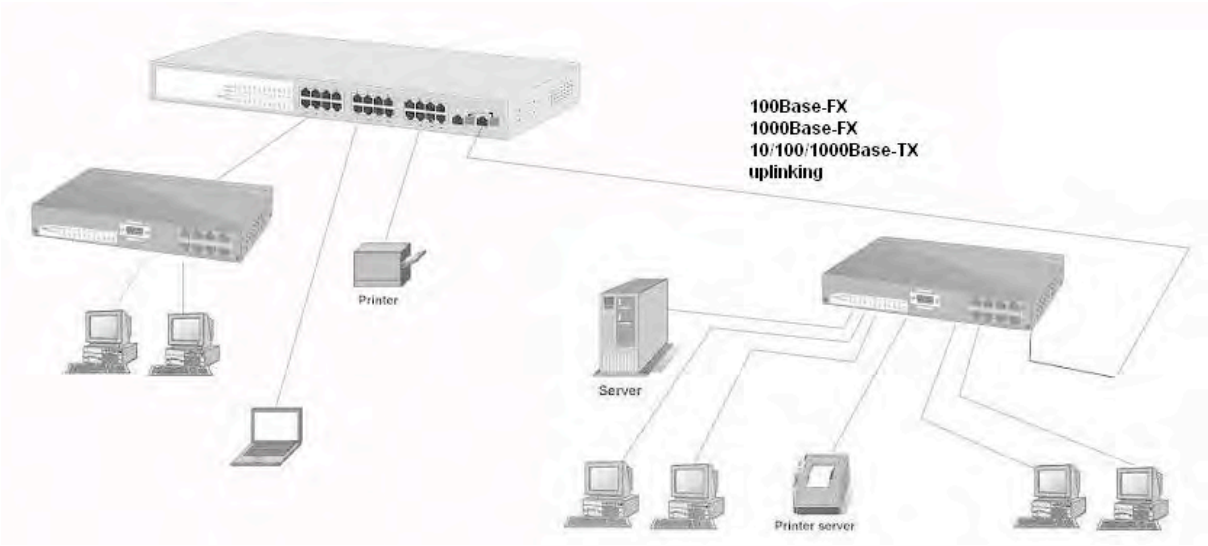
4.1 Desktop Application

The CWGE9MS managed Ethernet switch is designed to be a desktop size switch that is an ideal solution for small workgroup. The switch can be used as a standalone switch to which personal computers, server, printer server are directly connected to form small workgroup.



4.2 Segment Application

For enterprise networks where large data broadcast are constantly processed, this switch is suitable for department user to connect to the corporate backbone.

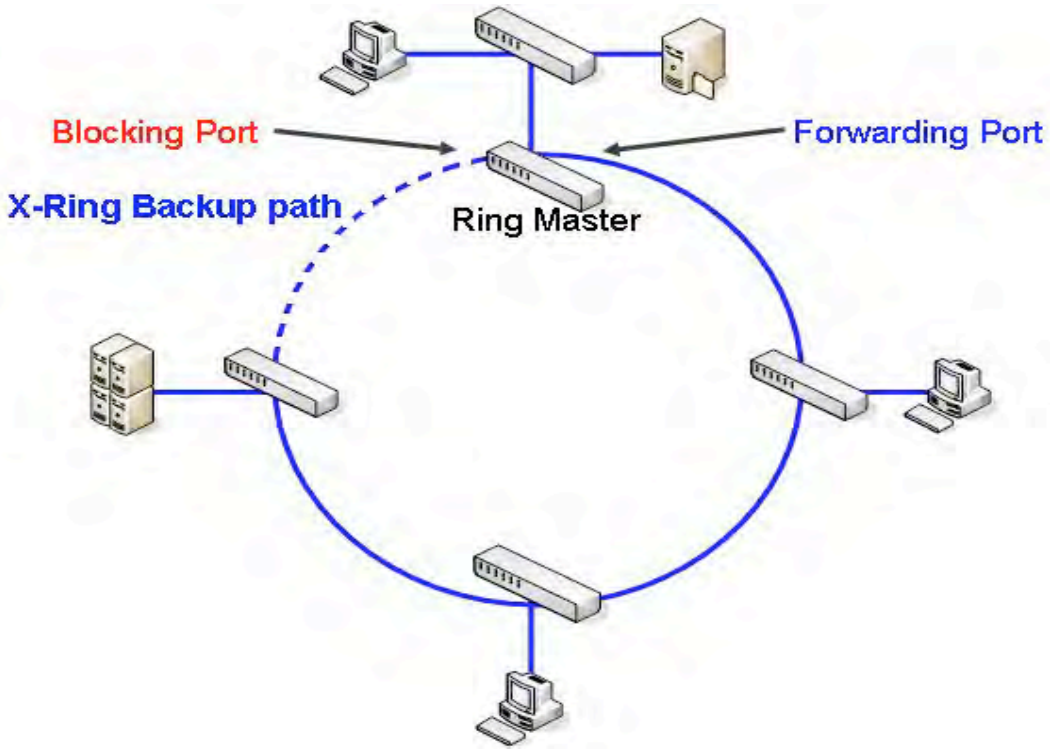


You can use the CWGE9MS managed Ethernet switch to connect PCs, workstations, and servers to each other by connecting these devices directly to the switch. All the devices in this network can communicate with each other. Connecting servers to the backbone switch allow other users to access the server's data.

The switch automatically learns node address, which are subsequently used to filter and forward all traffic based on the destination address. You can use any of the RJ45 port of the CWGE9MS managed Ethernet switch to connect with another Switch or Hub to interconnect each of your small-switched workgroups to form a larger switched network.

4.3 X-Ring Application

This industrial switch supports the X-Ring protocol that can help the network system to recovery from network connection failure within 20ms, making the network system more reliable. The X-Ring algorithm is similar to spanning tree protocol (STP) algorithm but the recovery time is faster than STP. The following figure is a sample X-Ring configuration.



[NOTE]

When the X-Ring function is enabled, the user must disable the RSTP. The X-Ring function and RSTP function cannot operate simultaneously.

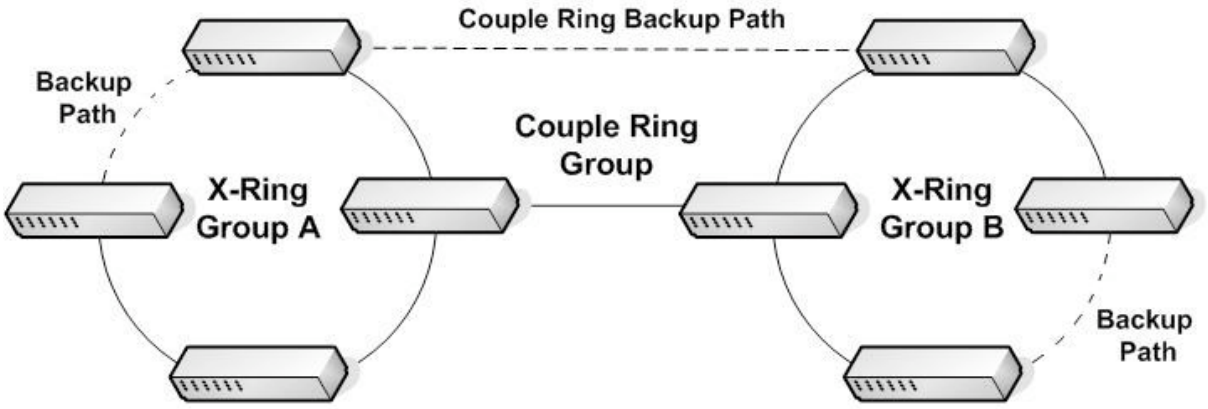
With X-Ring topology, every switch enables the X-Ring function and assigns two member ports in the ring. Only one switch in the X-Ring group would be the backup switch with one of the two member ports' being a backup port then switches are called working switches' working ports. When the network connection fails, the backup port will automatically become a working port to the failure. In the X-Ring group, switches are setting in "slave mode" by default, but one must be the "master mode". If there are 2 or more switches in the master mode, then software will automatically select the switch with lowest MAC address number as the ring master. The ringmaster has the rights to negotiate and command to other switches in the X-Ring group.

If a link fails the ringmaster is alerted and invokes its secondary port to rebuild the

network detection of the failed link's activation of the master's backup link and address table. If the failed link is restored, the ring slaves will alert the ringmaster to restore normal operation by disabling the backup link on the network in less than 300ms.

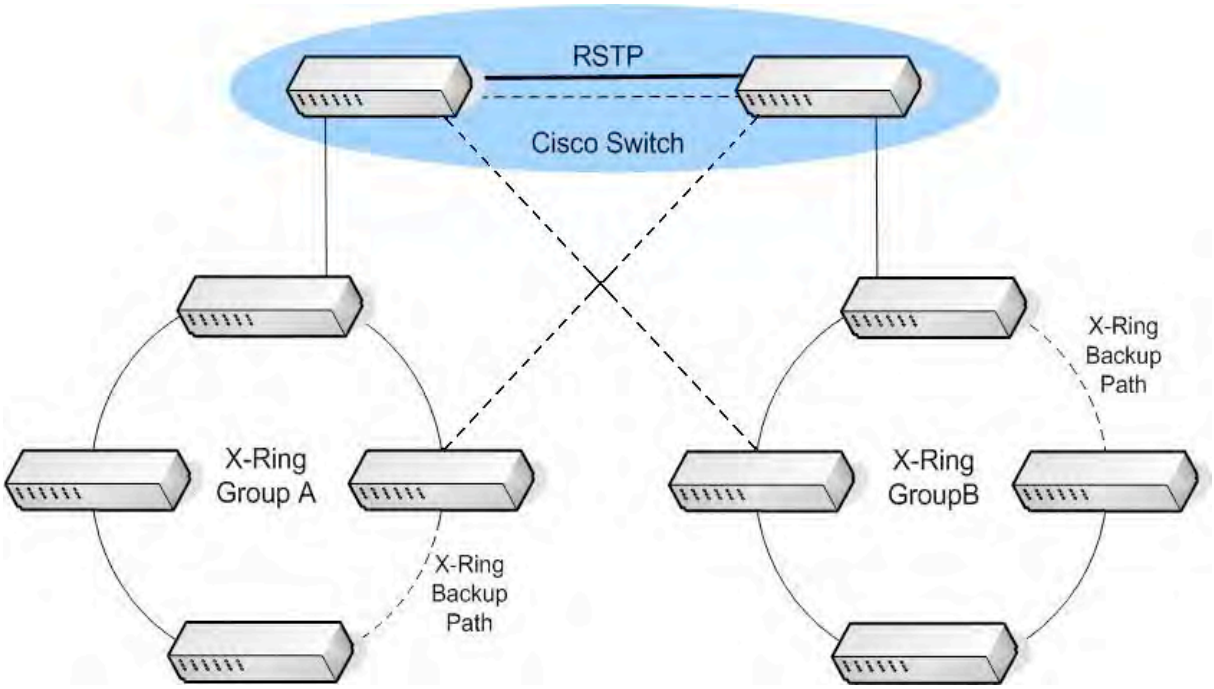
4.4 Coupling Ring Application

Within the network there may be more than one X-Ring group. By using the coupling ring function, it can connect each X-Ring for redundant backup. It can ensure the transmission between two ring groups will not fail. The following figure is a sample of a coupling ring application. The couple ring consists of four switches—switch 1 through switch 4 that are connected to each other via the paths in red. Please note that the Coupling Ring Backup Path between switch 1 and switch 3 is blocked; it will work only when the path between switch 2 and switch 4 is broken or disconnected.



4.5 Dual Homing Application

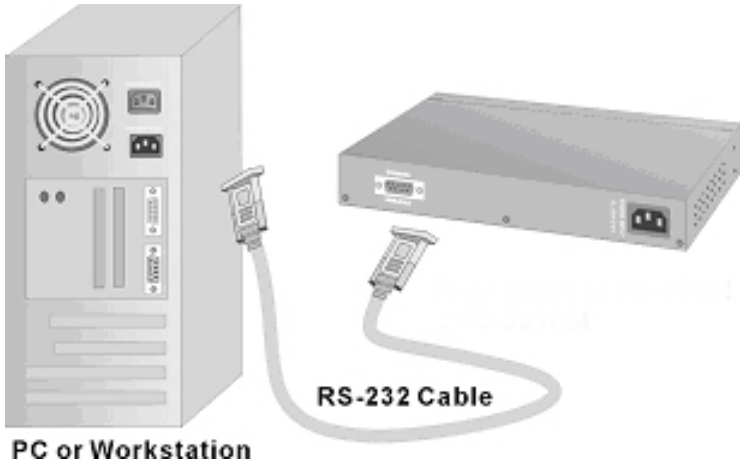
It provides the connection loss from between X-Ring group and an upper level/core switch. Assign two ports to be the Dual Homing port that is backup port in the X-Ring group. The Dual Homing function only works when the X-Ring function is active. Each X-Ring group only has one Dual Homing port.


RSTP
Cisco Switch
X-Ring
Group A
X-Ring
Backup
Path
X-Ring
Backup
Path
X-Ring
GroupB

Chapter 5 Console Management

5.1 Connecting to the Console Port

Use the supplied RS-232 cable to connect a terminal or PC to the console port. The terminal or PC to be connected must support the terminal emulation program.

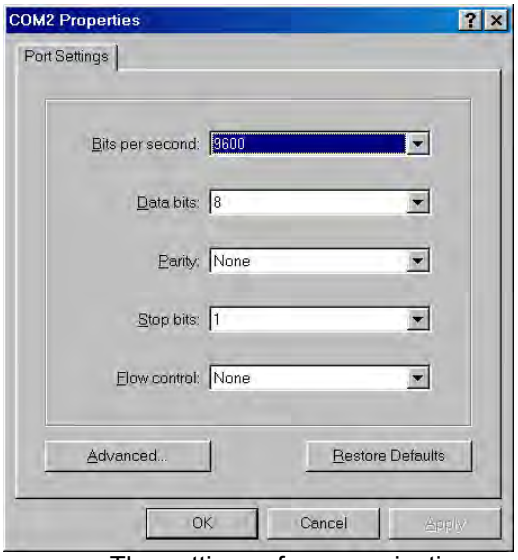


Connecting the switch to a terminal via RS-232 cable

5.2 Login in the Console Interface

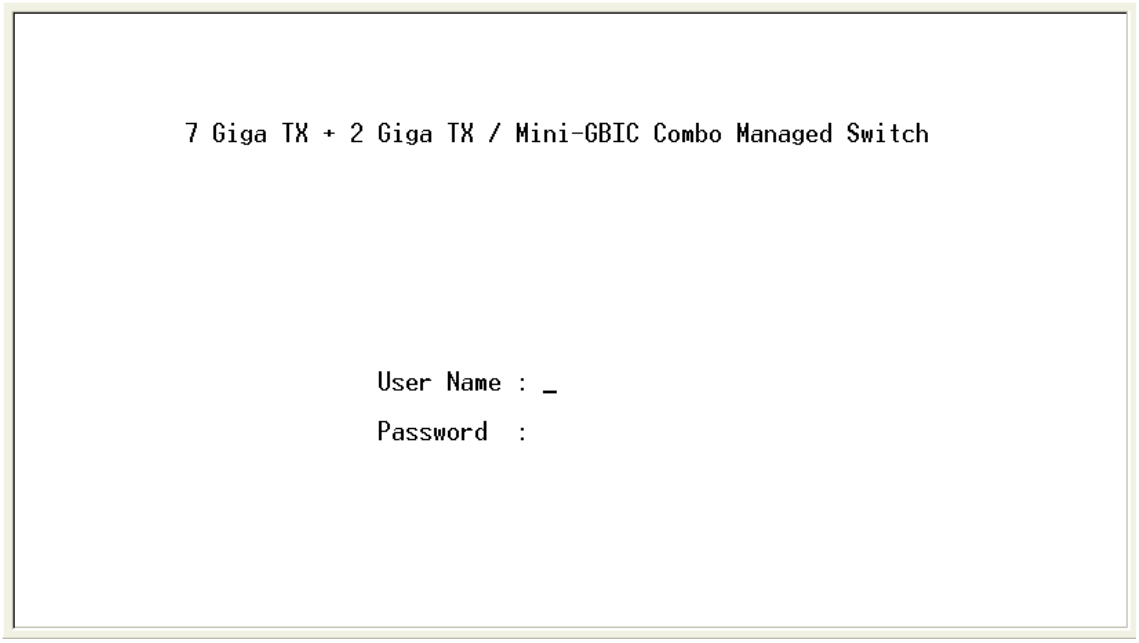
When the connection between Switch and PC is ready, turn on the PC and run a terminal emulation program or Hyper Terminal and configure its communication parameters to match the following default characteristics of the console port:

Baud Rate: 9600 bps
Data Bits: 8
Parity: none
Stop Bit: 1
Flow control: None



The settings of communication parameters

After finished the parameter settings, select "**OK**". When the blank screen shows up, press Enter key to bring out the login prompt. Key in the "**admin**" (default value) for the both User name and Password (use **Enter** key to switch), then press Enter key and the Main Menu of console management appears. Please see below figure for login screen.



Console login interface

5.3 CLI Management

The system supports two types of console management – CLI command. After you login to the system, you will see a command prompt. To enter CLI management interface, enter "**enable**" command. The following table lists the CLI commands and description.

Commands Level

Modes	Access Method	Prompt	Exit Method	About This Mode1
User EXEC	Begin a session with your switch.	switch>	Enter logout or quit.	The user commands available at the user level are a subset of those available at the privileged level. Use this mode to • Perform basic tests. • Display system information.
Privileged EXEC	Enter the enable command while in user EXEC mode.	switch#	Enter disable to exit.	The privileged command is advance mode Privileged this mode to • Display advance function status • Save configures
Global Configuration	Enter the configure command while in privileged EXEC mode.	switch (config)#	To exit to privileged EXEC mode, enter exit or end	Use this mode to configure parameters that apply to your switch as a whole.

VLAN database	Enter the vlan database command while in privileged EXEC mode.	switch (vlan)#	To exit to user EXEC mode, enter exit.	Use this mode to configure VLAN-specific parameters.
Interface configuration	Enter the interface command (with a specific interface) while in global configuration mode	switch (config-if)#	To exit to global configuration mode, enter exit. To exit to privileged EXEC mode, enter end.	Use this mode to configure parameters for the switch and Ethernet ports.

Chapter 6 Web-Based Management

This section introduces the configuration and functions of the Web-based management.

6.1 About Web-based Management

Inside the CPU board of the switch exists an embedded HTML web site residing in flash memory. It offers advanced management features and allow users to manage the switch from anywhere on the network through a standard browser such as Microsoft Internet Explorer.

The Web-Based Management supports Internet Explorer 5.0. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.

[NOTE]: By default, IE5.0 or later version does not allow Java Applets to open sockets. The user has to explicitly modify the browser setting to enable Java Applets to use network ports.

6.2 Preparing for Web Management

Before using web management, you can use console to login to the switch and check the default IP Address of the switch. Please refer to the **Console Management** Chapter for console login information. If you need to change the IP address the first time, you can use the console management mode to modify it. The default value is as below:

IP Address: **192.168.10.1**

Subnet Mask: **255.255.255.0**

Default Gateway: **192.168.10.254**

User Name: **admin** Password: **admin**

6.3 System Login

1. Launch the Internet Explorer on the PC
2. Key in “http:// “+” the IP address of the switch”, and then Press “**Enter**”.

Uniform Resource Locator

3. The login screen appears right after.
4. Key in the user name and password. The default user name and password are the same as ‘**admin’**
5. Press **Enter** or select **OK** button, and then the home screen of the Web-based management shows up.

Connect to 192.168.10.1
The server 192.168.10.1 at index.htm requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
admin
Password:
Remember my password
OK
Cancel

Login screen

6.4 System Information

Assign the system name and location and view the system information.

- **System Name:** Assign the system name of the switch (The maximum length is 64 bytes)
- **System Description:** Describes the switch.
- **System Location:** Assign the switch physical location (The maximum length is 64 bytes).
- **System Contact:** Enter the name of contact person or organization.
- **Firmware Version:** Displays the switch's firmware version
- **Kernel Version:** Displays the kernel software version
- **MAC Address:** Displays the unique hardware address assigned by manufacturer (default)
- And than, select

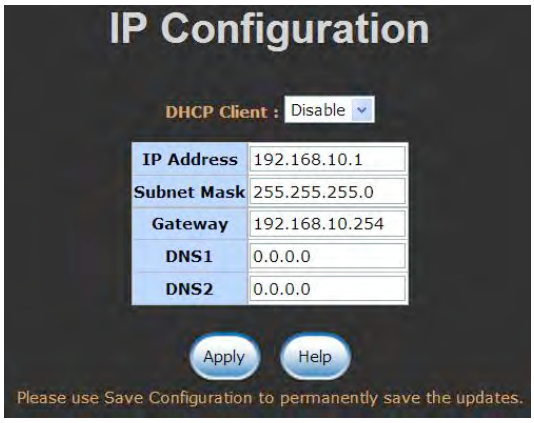
button.

6.5 IP Configuration

User can configure the IP Settings and DHCP client function here.

- **DHCP Client:** Enable or disable the DHCP client function. When DHCP client function is enabled, the industrial switch will be assigned an IP address from the network DHCP server. The default IP address will be replaced by the assigned IP address on DHCP server. After the user selects the **Apply** button, a popup dialog box shows up. It is to inform the user that when the DHCP client is enabled, the current IP address will be lost and user should find the new IP address on the DHCP server.
- **IP Address:** Assign the IP address that the network is using. If DHCP client function is enabled, and then the user does not need to assign the IP address. The network DHCP server will assign the IP address displaying in this column for the industrial switch. The default IP is 192.168.10.1.

- **Subnet Mask:** Assign the subnet mask to the IP address. If DHCP client function is enabled, and then the user does not need to assign the subnet mask.
- **Gateway:** Assign the network gateway for the industrial switch. The default gateway is 192.168.10.254.
- **DNS1:** Assign the primary DNS IP address.
- **DNS2:** Assign the secondary DNS IP address.
- And then, select



IP configuration interface

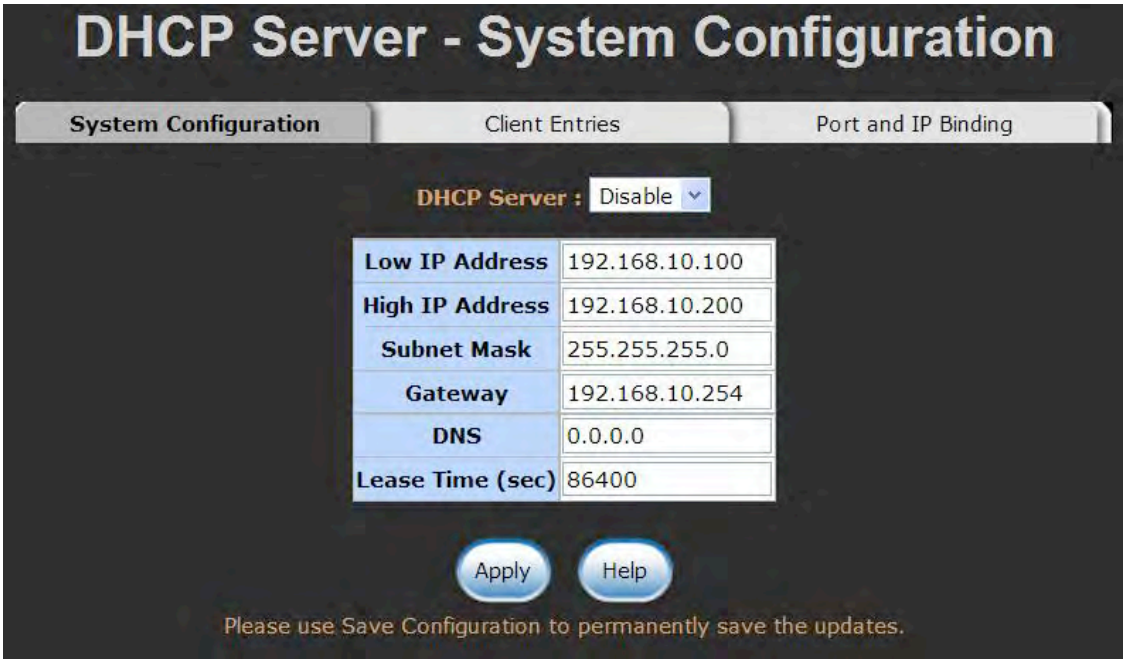
6.6 DHCP Server

DHCP is the abbreviation of Dynamic Host Configuration Protocol that is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses. Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP Address.

The system provides the DHCP server function. Enable the DHCP server function; the switch system will be a DHCP server.

6.6.1 System configuration

- **DHCP Server:** Enable or Disable the DHCP Server function. Enable—the switch will be the DHCP server on your local network.
- **Low IP Address:** Type in an IP address. Low IP address is the beginning of the dynamic IP range. For example, dynamic IP is in the range between 192.168.1.100 ~ 192.168.1.200. In contrast, 192.168.1.100 is the Low IP address.
- **High IP Address:** Type in an IP address. High IP address is the end of the dynamic IP range. For example, dynamic IP is in the range between 192.168.1.100 ~ 192.168.1.200. In contrast, 192.168.1.200 is the High IP address.
- **Subnet Mask:** Type in the subnet mask of the IP configuration.
- **Gateway:** Type in the IP address of the gateway in your network.
- **DNS:** Type in the Domain Name Server IP Address in your network.
- **Lease Time (sec):** It is the time period that system will reset the dynamic IP assignment to ensure the dynamic IP will not been occupied for a long time or the server doesn't know that the dynamic IP is idle.
- And then, select



DHCP Server Configuration interface

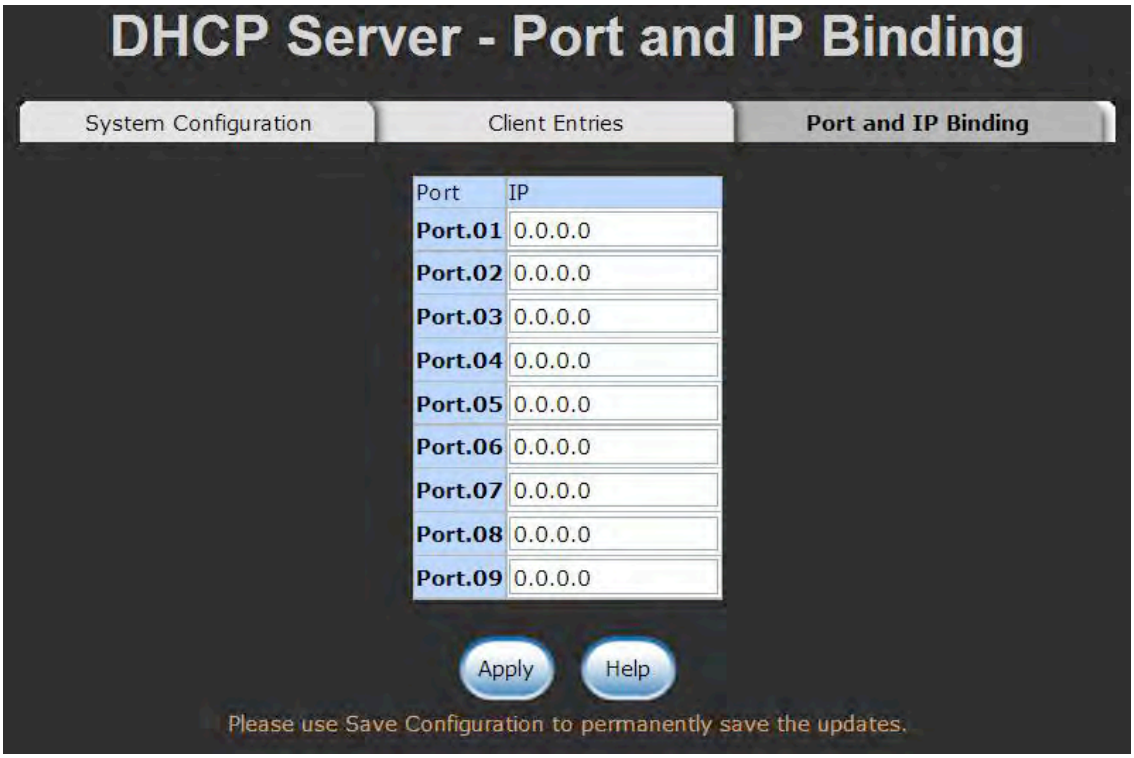
6.6.2 Client Entries

When the DHCP server function is active, the system will collect the DHCP client information and displays it at this tab.

DHCP Client Entries interface

6.6.3 Port and IP Bindings

Assign the dynamic IP address to the port. When the device is connecting to the port and asks for IP assigning, the system will assign the IP address that has been assigned before to the connected device.



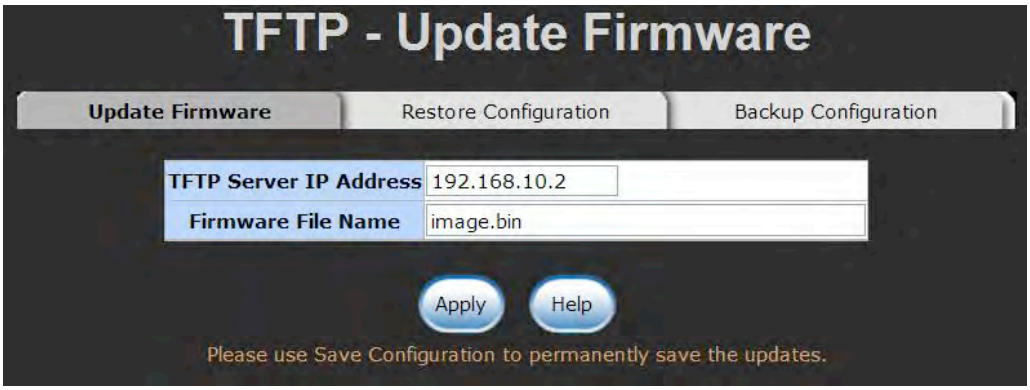
Port and IP Bindings interface

6.7 TFTP

6.7.1 Update Firmware

It provides the functions that allow user to update the switch firmware. Before updating, make sure the TFTP server is ready and the firmware image is located on the TFTP server.

1. **TFTP Server IP Address:** Type in your TFTP server IP.
2. **Firmware File Name:** Type in the name of firmware image.
3. Select Apply.

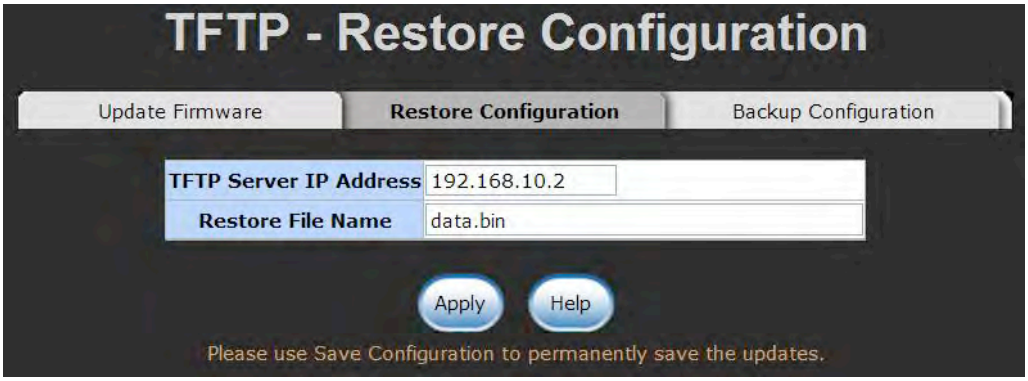


Update Firmware interface

6.7.2 Restore Configuration

You can restore the configuration from TFTP server. Before doing that, you must put the image file on TFTP server first and the switch will download back the flash image.

1. **TFTP Server IP Address:** Type in the TFTP server IP.
2. **Restore File Name:** Type in the correct file name for restoring.
3. Select Apply.



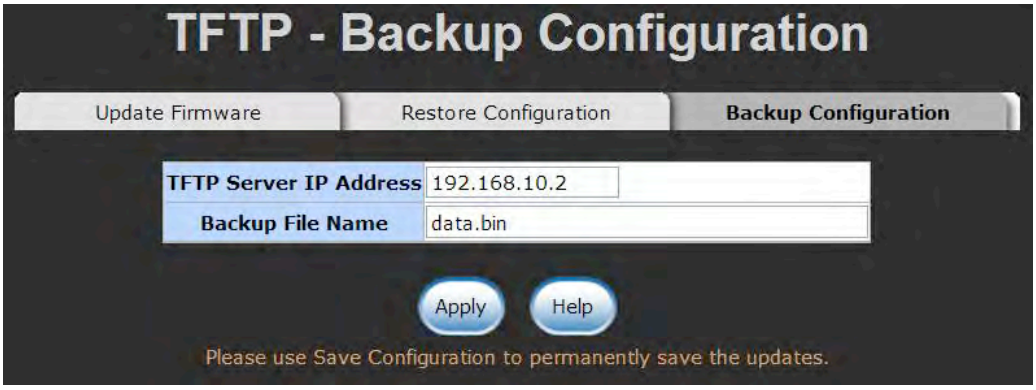
Restore Configuration interface

6.7.3 Backup Configuration

You can save the current configuration from flash ROM to TFTP server for restoring later.

1. **TFTP Server IP Address:** Type in the TFTP server IP.
2. **Backup File Name:** Type in the file name.
3. Select

.



Backup Configuration interface

6.8 System Event Log

6.8.1 Syslog Configuration

Configure the system event mode to collect system log.

1. **Syslog Client Mode:** Select the system log mode—**Client Only**, **Server Only**, or **Both**.
2. **System Log Server IP Address:** Assign the system log server IP.
3. When Syslog Client Mode is set as **Client Only**, the system event log will only be reserved in the switch's RAM until next reboot. When Syslog Client Mode is set as **Server Only**, the system log will only be sent to the syslog server and you have to type the IP address in the Sysylog Server IP Address column. If the Syslog Client Mode is set as **Both**, the system log will be reserved in the switch's RAM and sent to server.
4. Select

to refresh the events log.
5. Select

to clear all current events log.
6. After configuring, select

button.

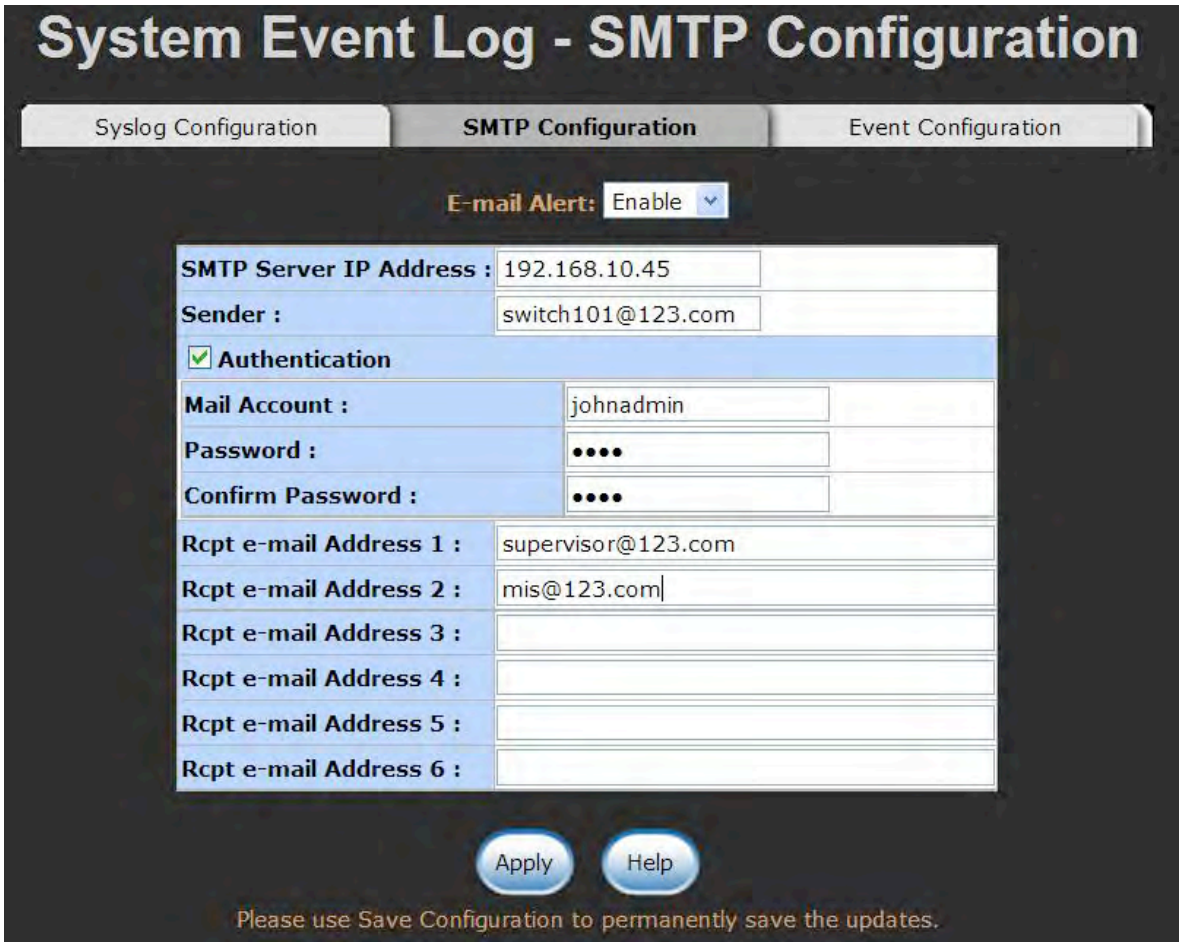
Syslog Configuration interface

6.8.2 SMTP Configuration

You can set up the mail server IP, mail account, password, and forwarded email account for receiving the event alert.

1. **Email Alert:** Enable or disable the email alert function.
2. **SMTP Server IP:** Set up the mail server IP address (when **Email Alert** enabled, this function will then be available).
3. **Sender:** Type in an alias of the switch in complete email address format, e.g. switch101@123.com, to identify where the event log comes from.

4. **Authentication:** Select the checkbox to enable this function, configuring the email account and password for authentication (when **Email Alert** enabled, this function will then be available).
5. **Mail Account:** Set up the email account, e.g. johnadmin, to receive the alert. It must be an existing email account on the mail server, which you had set up in **SMTP Server IP Address** column.
6. **Password:** Type in the password to the email account.
7. **Confirm Password:** Reconfirm the password.
8. **Rcpt e-mail Address 1 ~ 6:** You can also assign up to 6 e-mail accounts to receive the alert.
9. Select Apply button.


System Event Log - SMTP Configuration
Syslog Configuration
SMTP Configuration
Event Configuration
E-mail Alert: Enable
SMTP Server IP Address : 192.168.10.45
Sender : switch101@123.com
Authentication
Mail Account : johnadmin
Password : ••••
Confirm Password : ••••
Rcpt e-mail Address 1 : supervisor@123.com
Rcpt e-mail Address 2 : mis@123.com
Rcpt e-mail Address 3 :
Rcpt e-mail Address 4 :
Rcpt e-mail Address 5 :
Rcpt e-mail Address 6 :
Apply
Help
Please use Save Configuration to permanently save the updates.

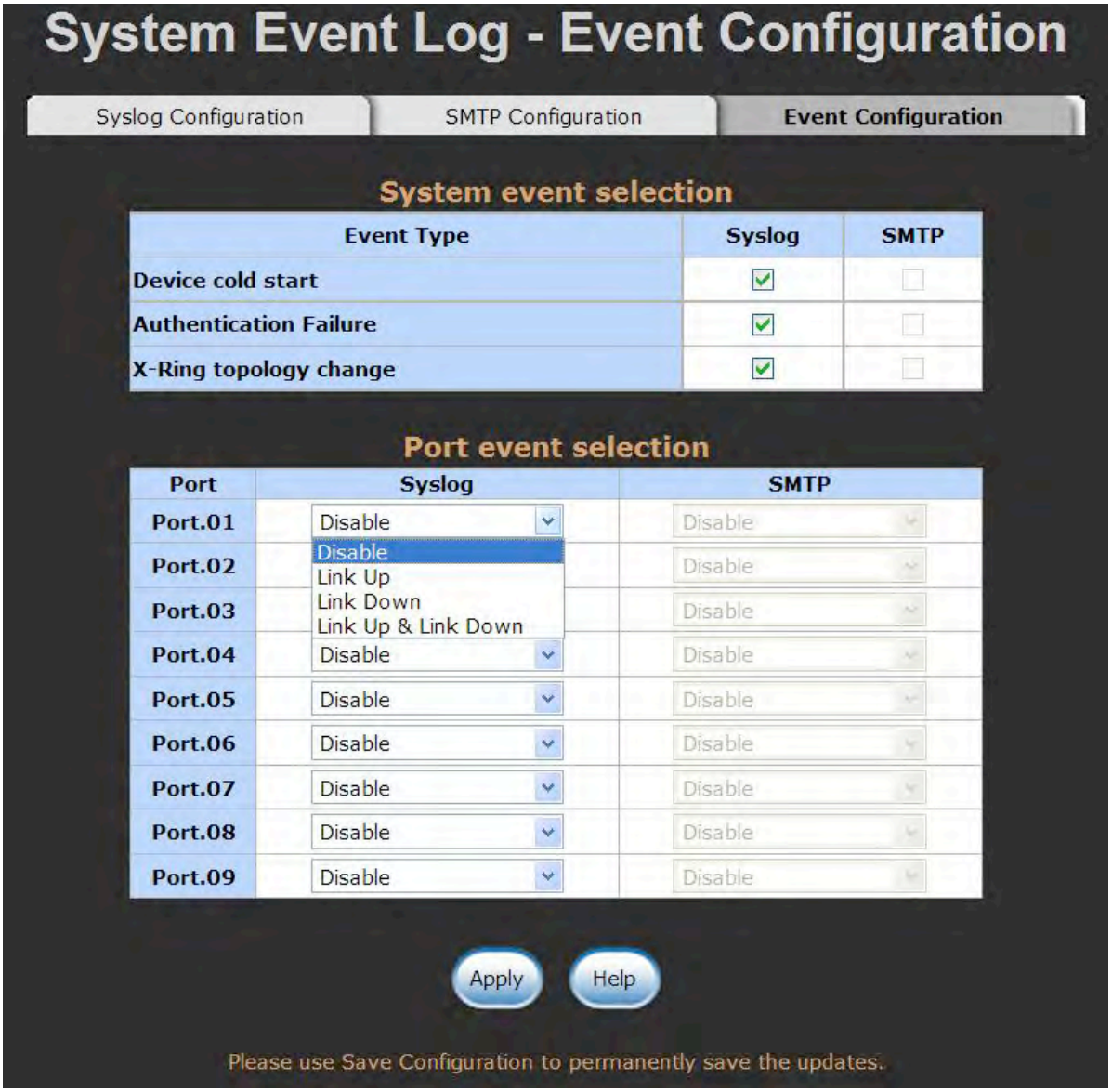
SMTP Configuration interface

6.8.3 Event Configuration

When the **Syslog**/**SMTP** checkbox is marked, the event log will be sent to system log server/SMTP server. Also, per port log (link up, link down, and both) events can be sent to the system log server/SMTP server with the respective checkbox selected. After configuring, select

to have the setting taken effect.

- **System event selection:** There are 4 event types—Device cold start, Device warm start, Authentication Failure, and X-ring topology change. Before you can select the checkbox of each event type, the Syslog Client Mode column on the Syslog Configuration tab/E-mail Alert column on the SMTP Configuration tab must be enabled first.
  - **Device cold start:** When the device executes cold start action, the system will issue a log event.
  - **Device warm start:** When the device executes warm start, the system will issue a log event.
  - **Authentication Failure:** When the SNMP authentication fails, the system will issue a log event.
  - **X-ring topology change:** When the X-ring topology has changed, the system will issue a log event.
- **Port event selection:** Also, before the drop-down menu items are available, the Syslog Client Mode column on the Syslog Configuration tab and the E-mail Alert column on the SMTP Configuration tab must be enabled first. Those drop-down menu items have 3 selections—Link UP, Link Down, and Link UP & Link Down. Disable means no event will be sent to the system log server/SMTP server.
  - **Link UP:** The system will issue a log message when port connection is up only.
  - **Link Down:** The system will issue a log message when port connection is down only.
  - **Link UP & Link Down:** The system will issue a log message when port connection is up and down.



Event Configuration interface

6.9 SNTP Configuration

You can configure the SNTP (Simple Network Time Protocol) settings. The SNTP allows you to synchronize switch clocks in the Internet.

1. **SNTP Client:** Enable/disable SNTP function to get the time from the SNTP server.
2. **Daylight Saving Time:** Enable/disable daylight saving time function. When daylight saving time is enabled, you need to configure the daylight saving time period.
3. **UTC Timezone:** Set the switch location time zone. The following table lists the different location time zone for your reference.

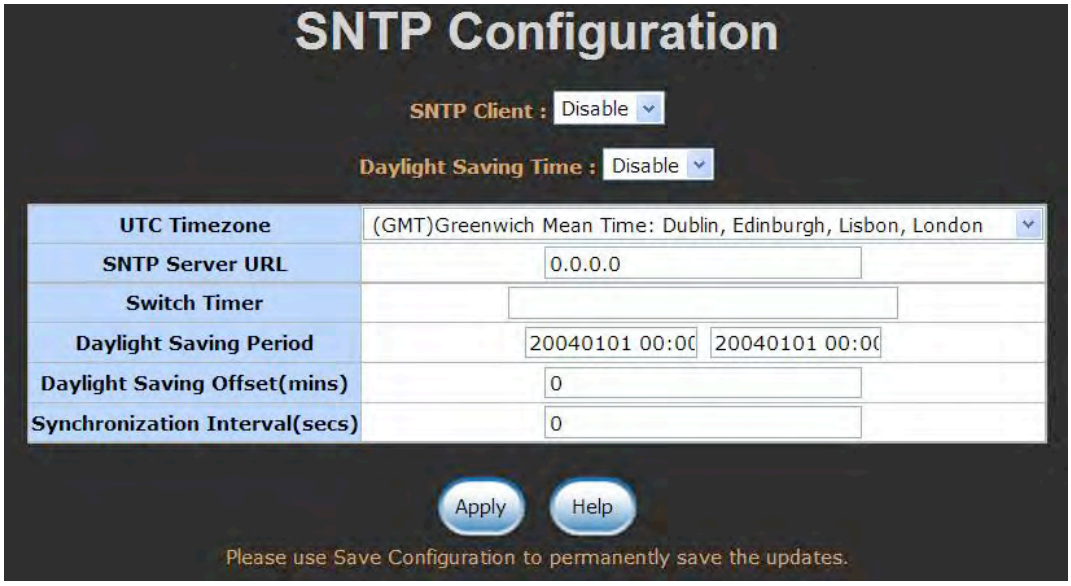
Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	1 am

CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm
BT - Baghdad, USSR Zone 2	+3 hours	3 pm
ZP4 - USSR Zone 3	+4 hours	4 pm
ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm
WAST - West Australian Standard	+7 hours	7 pm
CCT - China Coast, USSR Zone 7	+8 hours	8 pm
JST - Japan Standard, USSR Zone 8	+9 hours	9 pm
EAST - East Australian Standard GST Guam Standard, USSR Zone 9	+10 hours	10 pm
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

4. **SNTP Sever URL:** Set the SNTP server IP address.
5. **Switch Timer:** Displays the current time of the switch.
6. **Daylight Saving Period:** Set up the Daylight Saving beginning time and Daylight Saving ending time. Both will be different in every year.
7. **Daylight Saving Offset (mins):** For non-US and European countries, specify the amount of time for day light savings.

8. Select

.



SNTP Configuration interface

6.10 IP Security

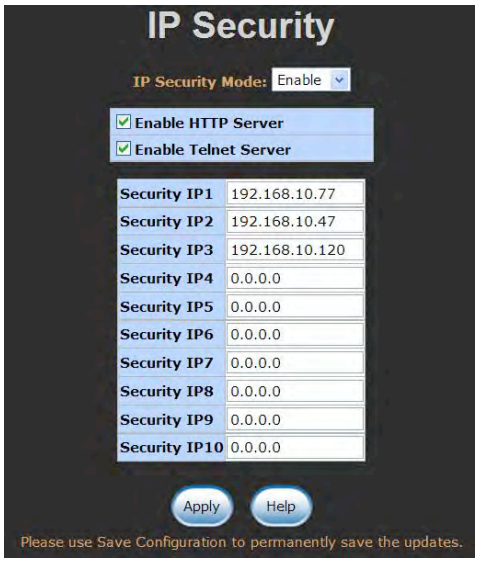
The IP security function allows the user to assign 10 specific IP addresses that have permission to access the switch through the web browser for the securing switch management.

- **IP Security Mode:** When this option is in **Enable** mode, the **Enable HTTP Server** and **Enable Telnet Server** checkboxes will then be available.
- **Enable HTTP Server:** When this checkbox is selected, the IP addresses among Security IP1 ~ IP10 will be allowed to access this switch via HTTP service.
- **Enable Telnet Server:** When this checkbox is selected, the IP addresses among Security IP1 ~ IP10 will be allowed to access this switch via telnet service.
- **Security IP 1 ~ 10:** The system allows the user to assign up to 10 specific IP addresses for access security. Only these 10 IP addresses can access and manage the switch through the HTTP/Telnet service.

- And then, select

button to apply the configuration.

[NOTE]	Remember to execute the “Save Configuration” action, otherwise the new configuration will lose when the switch powers off.

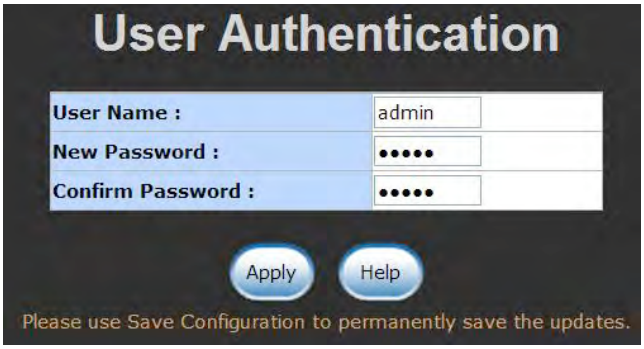


IP Security interface

6.11 User Authentication

Change web management login user name and password for the management security issue.

1. **User name:** Type in the new user name (The default is ‘admin’)
2. **Password:** Type in the new password (The default is ‘admin’)
3. **Confirm password:** Re-type the new password
4. And then, select



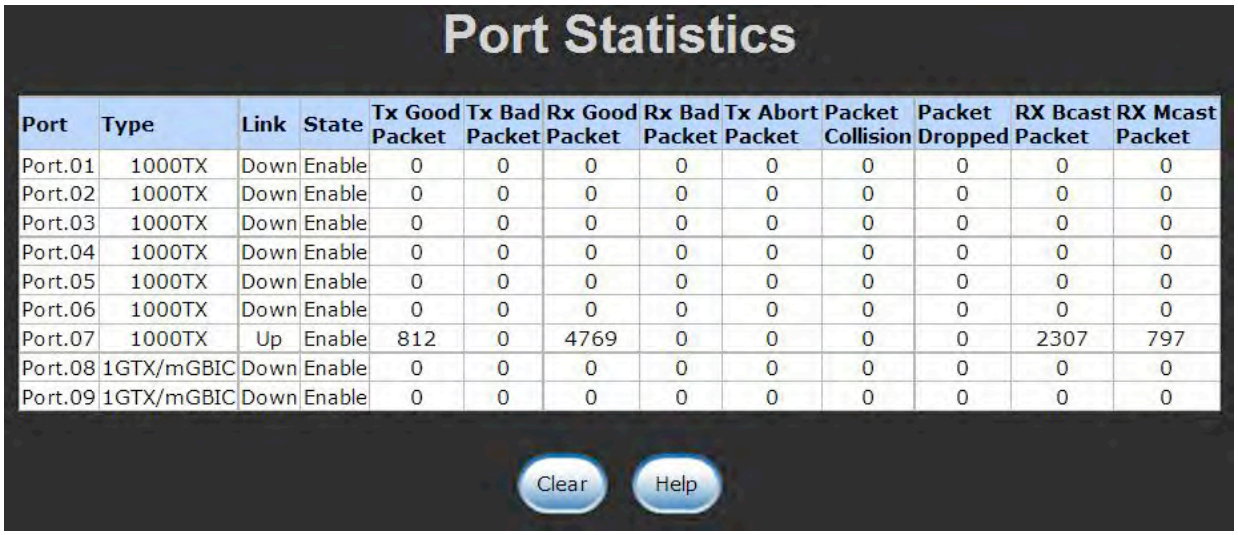
User Authentication interface

6.12 Port Statistics

The following information provides the current port statistic information.

- **Port:** Displays the port number.
- **Type:** Displays the media type of the port.
- **Link:** The status of linking—'**Up**' or '**Down**'.
- **State:** The user can set the state of the port as 'Enable' or 'Disable' via Port Control. When the state is disabled, the port will not transmit or receive any packet.
- **Tx Good Packet:** The counts of transmitting good packets via this port.
- **Tx Bad Packet:** The counts of transmitting bad packets (including undersize [< 64 bytes], oversize, CRC Align errors, fragments and jabbers packets) via this port.
- **Rx Good Packet:** The counts of receiving good packets via this port.
- **Rx Bad Packet:** The counts of receiving bad packets (including undersize [less than 64 bytes], oversize, CRC error, fragments and jabbers) via this port.
- **Tx Abort Packet:** The aborted packet while transmitting.
- **Packet Collision:** The counts of collision packet.
- **Packet Dropped:** The counts of dropped packet.
- **Rx Bcast Packet:** The counts of broadcast packet.
- **Rx Mcast Packet:** The counts of multicast packet.
- Select

button to clean all counts.


Port Statistics
Port Type Link State Tx Good Packet Tx Bad Packet Rx Good Packet Rx Bad Packet Tx Abort Packet Packet Collision Packet Dropped RX Bcast Packet RX Mcast Packet
Port.01 1000TX Down Enable 0 0 0 0 0 0 0 0 0
Port.02 1000TX Down Enable 0 0 0 0 0 0 0 0 0
Port.03 1000TX Down Enable 0 0 0 0 0 0 0 0 0
Port.04 1000TX Down Enable 0 0 0 0 0 0 0 0 0
Port.05 1000TX Down Enable 0 0 0 0 0 0 0 0 0
Port.06 1000TX Down Enable 0 0 0 0 0 0 0 0 0
Port.07 1000TX Up Enable 812 0 4769 0 0 0 0 2307 797
Port.08 1GTX/mGBIC Down Enable 0 0 0 0 0 0 0 0 0
Port.09 1GTX/mGBIC Down Enable 0 0 0 0 0 0 0 0 0
Clear
Help

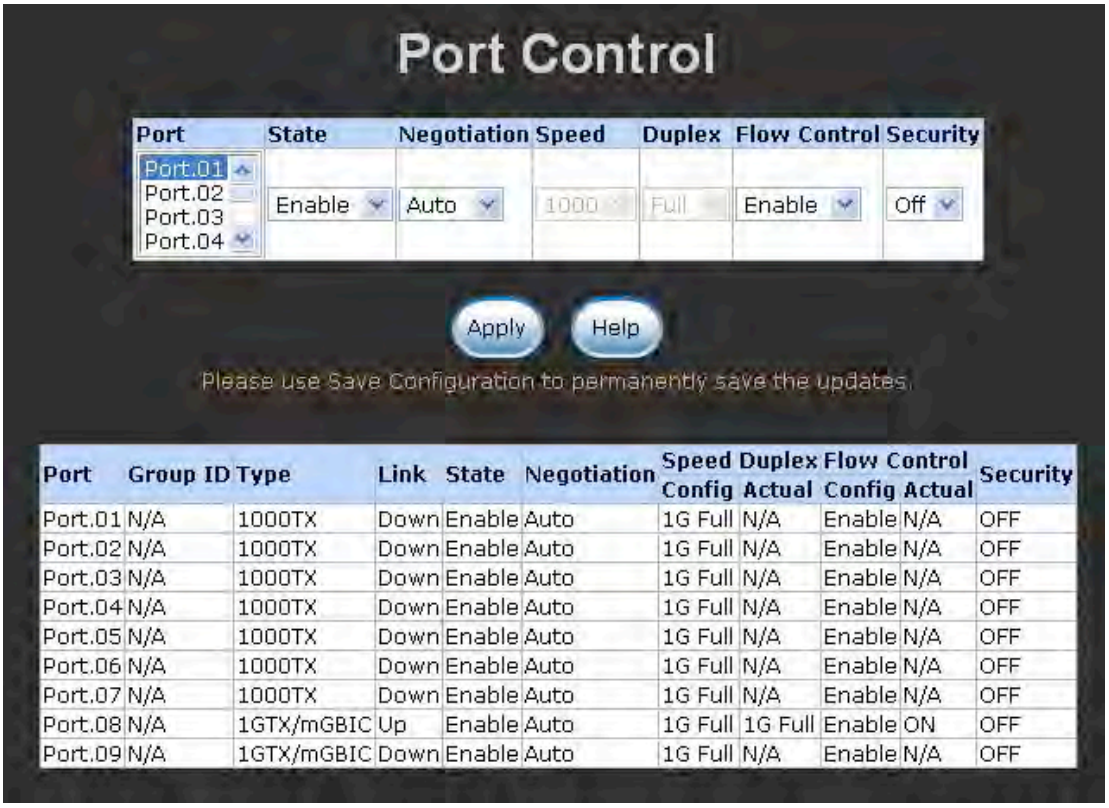
Port Statistics interface

6.13 Port Control

In Port control, you can view and set the operation mode of each port.

1. **Port:** Select the port that you want to configure.
2. **State:** Current port status. The port can be set to disable or enable mode. If the port state is set as 'Disable', it will not receive or transmit any packet.
3. **Negotiation:** Auto and Force. Being set as Auto, the speed and duplex mode are negotiated automatically. When you set it as Force, you have to assign the speed and duplex mode manually.
4. **Speed:** It is available for selecting when the Negotiation column is set as Force. When the Negotiation column is set as Auto, this column is read only.
5. **Duplex:** It is available for selecting when the Negotiation column is set as Force. When the Negotiation column is set as Auto, this column is read only.
6. **Flow Control:** Set flow control function as Enable or Disable. When enabled, once the device exceed the input data rate of another device as a result the receiving device will send a PAUSE frame which halts the transmission of the sender for a specified period of time. When disabled, the receiving device will drop the packet if too much to process.
7. **Security:** Once the Security selection is set as '**On**', any access from the device that connects to this port will be blocked unless the MAC address of the device is included in the static MAC address table. See the segment of Static MAC Table.
8. Select

button to make the configuration effective.


Port Control
Port
State
Negotiation
Speed
Duplex
Flow Control
Security
Port.01
Port.02
Port.03
Port.04
Enable
Auto
1000
Full
Enable
Off
Apply
Help
Please use Save Configuration to permanently save the updates.
Port Group ID Type Link State Negotiation Speed Config Duplex Actual Flow Control Config Flow Control Actual Security
Port.01 N/A 1000TX Down Enable Auto 1G Full N/A Enable N/A OFF
Port.02 N/A 1000TX Down Enable Auto 1G Full N/A Enable N/A OFF
Port.03 N/A 1000TX Down Enable Auto 1G Full N/A Enable N/A OFF
Port.04 N/A 1000TX Down Enable Auto 1G Full N/A Enable N/A OFF
Port.05 N/A 1000TX Down Enable Auto 1G Full N/A Enable N/A OFF
Port.06 N/A 1000TX Down Enable Auto 1G Full N/A Enable N/A OFF
Port.07 N/A 1000TX Down Enable Auto 1G Full N/A Enable N/A OFF
Port.08 N/A 1GTX/mGBIC Up Enable Auto 1G Full 1G Full Enable ON OFF
Port.09 N/A 1GTX/mGBIC Down Enable Auto 1G Full N/A Enable N/A OFF

Port Control interface

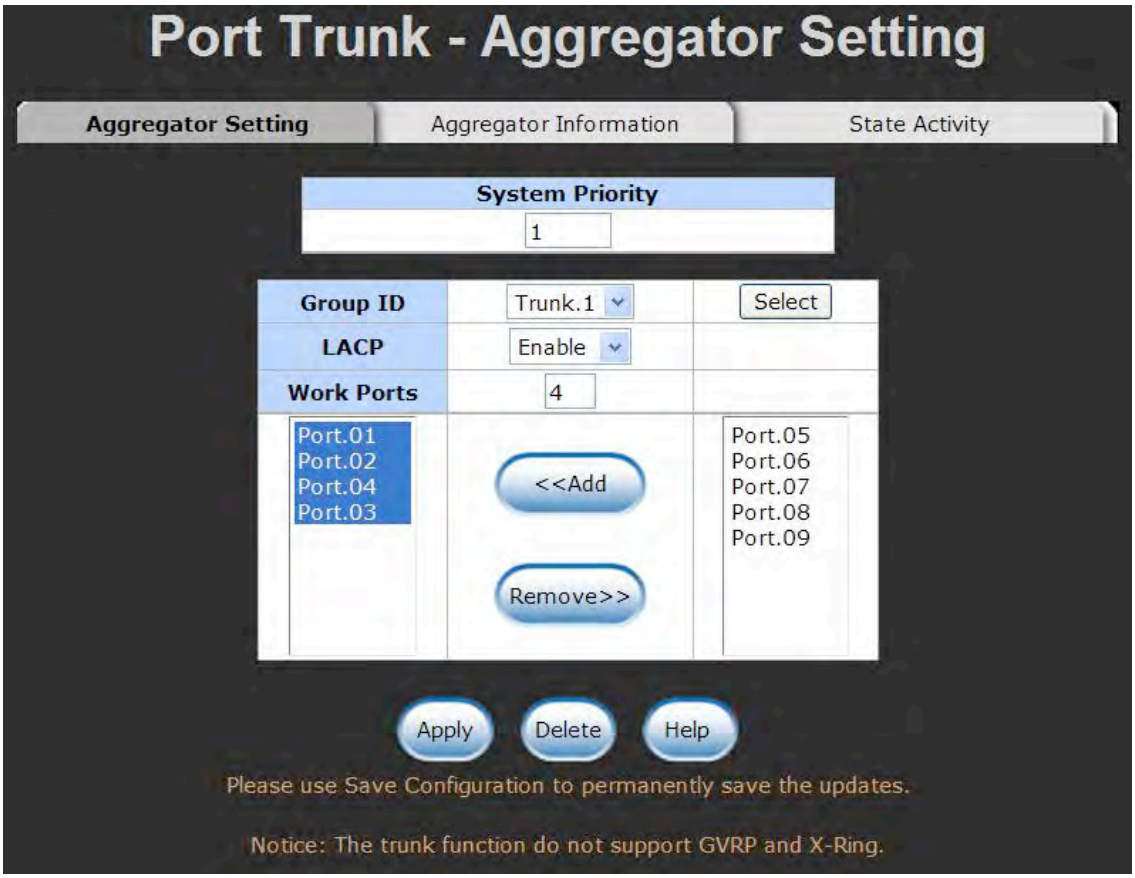
6.14 Port Trunk

The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs, move the link to that Link Aggregation Group, and enable its transmission and reception functions in an orderly manner. Link aggregation lets you group up to 4 ports into one dedicated connections. This feature can expand bandwidth to a device on the network. **LACP operation requires full-duplex mode,** more detail information refers to IEEE 802.3ad.

6.14.1 Aggregator setting

1. **System Priority:** A value that is used to identify the active LACP. The switch with the lowest value has the highest priority and is selected as the active LACP.
2. **Group ID:** There are four trunk groups to be selected. Choose the "**Group ID**" and select Select button.
3. **LACP:** When enabled, the trunk group is using LACP. A port that joins an LACP trunk group has to make an agreement with its member ports first. When disabled, the trunk group is a static trunk group. The advantage of having the LACP disabled is that a port joins the trunk group without any handshaking with its member ports. But member ports won't know that they should be aggregated together to form a logic trunk group.
4. **Work ports:** This column field allows the user to type in the total number of active port up to four. With LACP trunk group, you create a trunk group by connecting two or more switches (e.g. you assign four ports to be the members of the trunk group whose work ports column field is set as two). The exceed ports are standby (the **Aggregator Information** tab will show standby status on the exceed ports) and can be aggregated if work ports fail. If it is a static trunk group, the number of work ports must equal the total number of group member ports.
5. Select the ports to join the trunk group. The system allows four ports maximum to be aggregated in a trunk group. Select <<Add button to add the port that is focused to the left field. To remove unwanted ports, select the port and select Remove>> button.
6. When LACP enabled, you can configure LACP Active/Passive status for each port on State Activity page.
7. Select Apply button.

8. Use button to delete Trunk Group. Select the Group ID and select button.

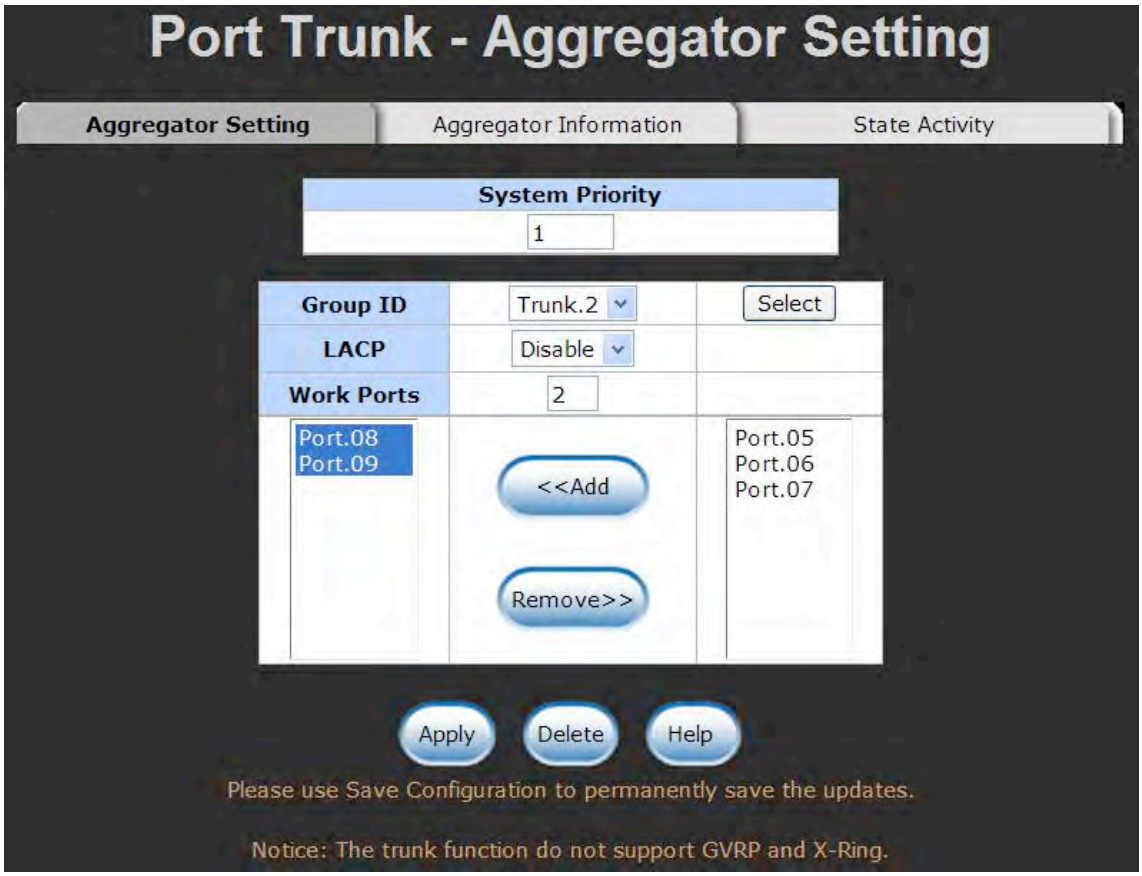


Port Trunk—Aggregator Setting interface (four ports are added to the left field with LACP enabled)

6.14.2 Aggregator Information

When you have setup the aggregator setting with LACP disabled, you will see the local static trunk group information here.

1. **Group Key:** Displays the trunk group ID.
2. **Port Member:** Displays the members of this static trunk group.



Port Trunk—Aggregator Setting interface (two ports are added to the left field with LACP disable)

Port Trunk – Aggregator Information interface

6.14.3 State Activity

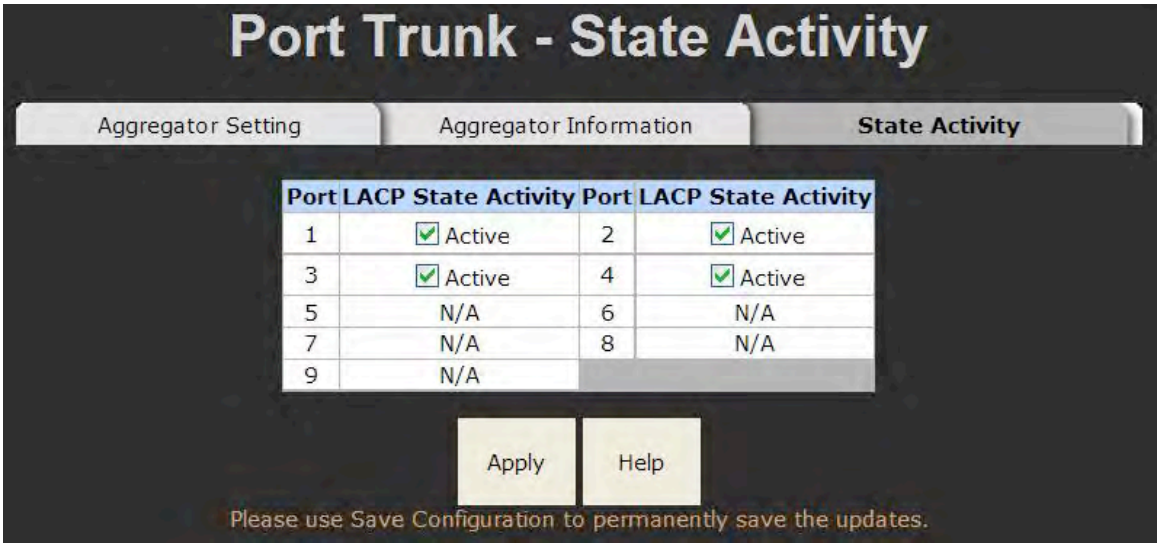
Having set up the LACP aggregator on the tab of Aggregator Setting, you can configure the state activity for the members of the LACP trunk group. You can select or cancel the checkbox beside the state display. When you remove the select mark to the port and select

button, the port state activity will change to **Passive**.

- **Active:** The port automatically sends LACP protocol packets.
- **Passive:** The port does not automatically send LACP protocol packets, and responds only if it receives LACP protocol packets from the opposite device.

[NOTE]

1. **A link** having either two active LACP nodes or one active node can perform dynamic LACP trunk.
2. **A link** having two passive LACP nodes will not perform dynamic LACP trunk because both ports are waiting for an LACP protocol packet from the opposite device.



Port Trunk – State Activity interface

6.15 Port Mirroring

The Port mirroring is a method for monitoring traffic in switched networks. Traffic through ports can be monitored by one specific port which means traffic goes in or out monitored (source) ports will be duplicated into mirroring (destination) port.

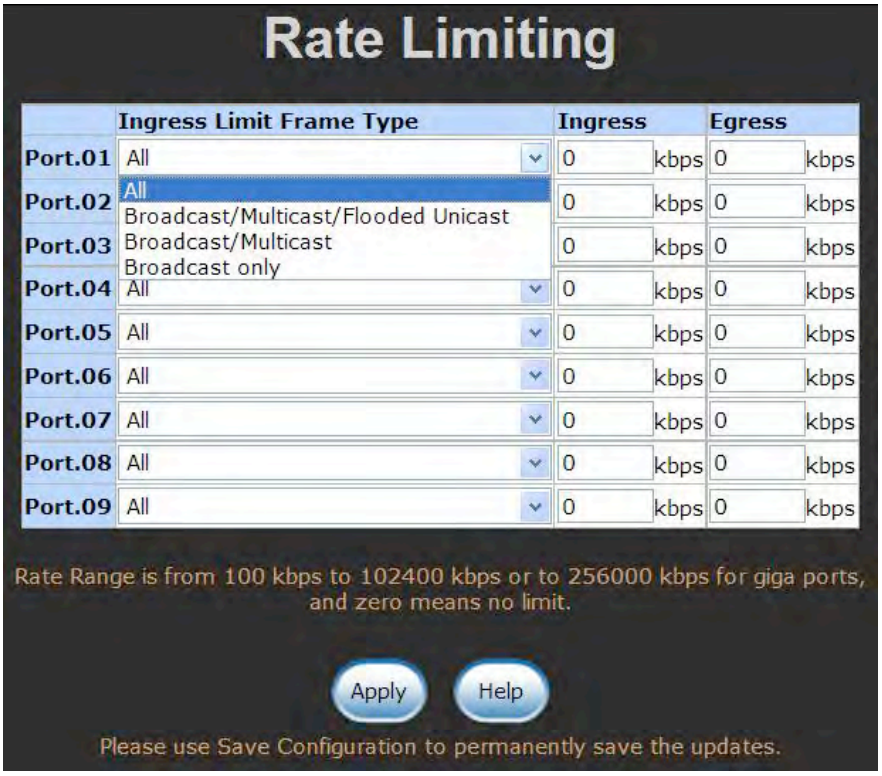
Port Trunk – Port Mirroring interface

- **Destination Port:** There is only one port can be selected to be the destination (mirroring) port for monitoring both RX and TX traffic which come from the source port. Or, use one of two ports for monitoring RX traffic only and the other one for TX traffic only. The user can connect the mirroring port to LAN analyzer or Netxray.
- **Source Port:** The ports that the user wants to monitor. All monitored port traffic will be copied to mirroring (destination) port. The user can select multiple source ports by selecting the **RX** or **TX** checkboxes to be monitored.
- And then, select

button.

6.16 Rate Limiting

You can set up every port's frame limitation type and bandwidth rate.



Rate Limiting interface

- **Ingress Limit Frame type:** Select the frame type you want to filter. The frame types have 4 options for selecting: **All, Broadcast/Multicast/Flooded Unicast, Broadcast/Multicast,** and **Broadcast only**.

  The four frame type options are for ingress frames limitation. The egress rate only supports '**All**' type.

- All the ports support port ingress and egress rate control. For example, assume port 1 is 10Mbps; the user can set the effective egress rate of port 1 as 1Mbps, ingress rate 500Kbps. The switch performs the ingress rate by packet counter to meet the specified rate.

  - **Ingress:** Enter the port effective ingress rate (The default value is "0").

- **Egress:** Enter the port effective egress rate (The default value is “0”).

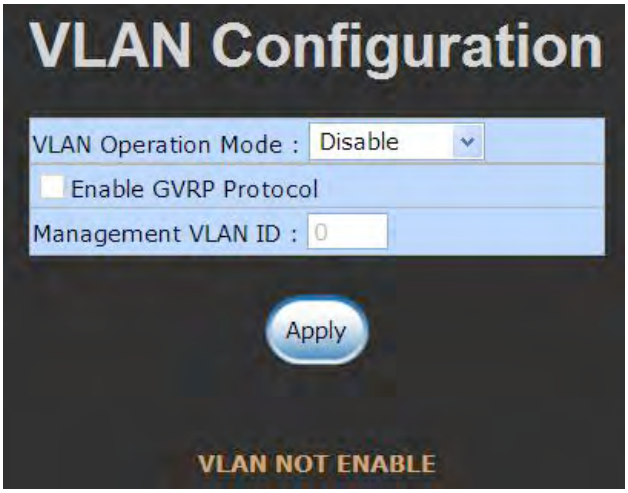
■ And then, select

to make the settings taken effect.

6.17 VLAN configuration

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain, which would allow you to isolate network traffic, so only the members of the same VLAN will receive traffic from the ones of the same VLAN. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plugged into the same switch physically.

The switch supports **Port-based** and **802.1Q** (tagged-based) VLAN. The default configuration of VLAN operation mode is “**Disable**”.



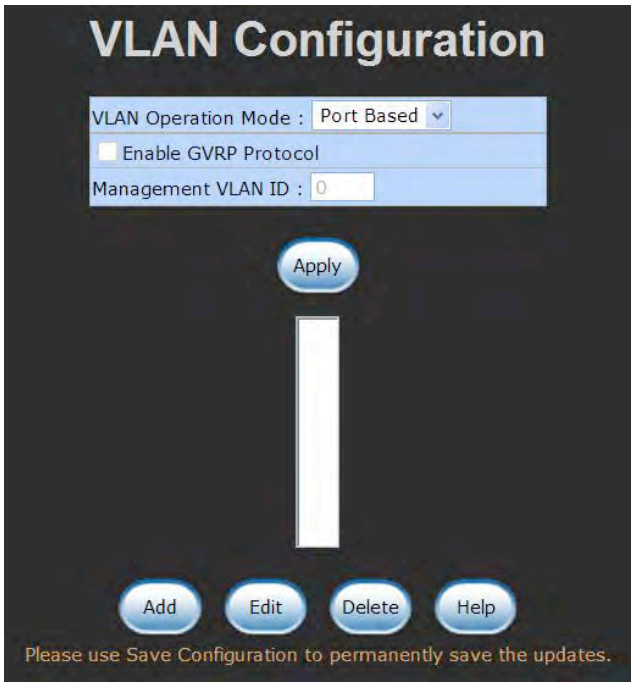
VLAN Configuration interface

6.17.1 Port-based VLAN

Packets can go among only members of the same VLAN group. Note all unselected

ports are treated as belonging to another single VLAN. If the port-based VLAN is enabled, the VLAN-tagging is ignored.

In order for an end station to send packets to different VLAN groups, it has to be either capable of tagging packets it sends with VLAN tags or attached to a VLAN-aware bridge that is capable of classifying and tagging the packet with different VLAN ID based on not only default PVID but also other information about the packet, such as the protocol.

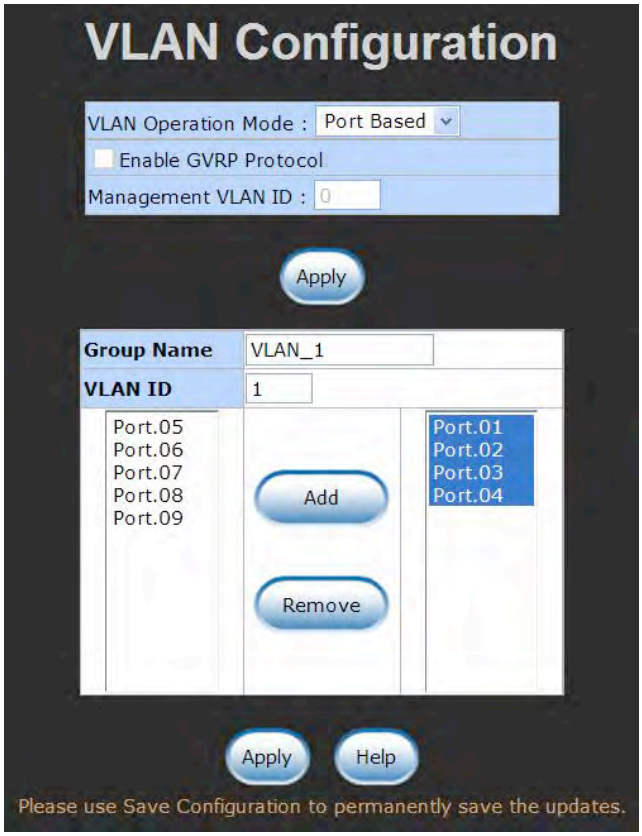


VLAN – Port Based interface

- Pull down the selection item and focus on **Port Based** then select

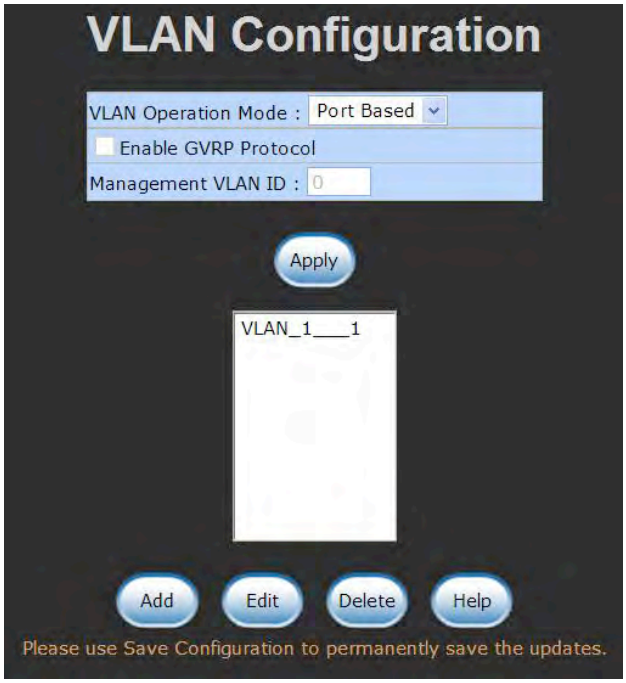
button to set the VLAN Operation Mode in **Port Based** mode.
- Select

button to add a new VLAN group.



VLAN—Port Based Add interface

- Enter the group name and VLAN ID. Add the port number having selected into the right field to group these members to be a VLAN group or remove any of them listed in the right field from the VLAN.
- And then, select button to have the settings taken effect.
- You will see the VLAN displays.



VLAN—Port Based Edit/Delete interface

- Use button to delete the VLAN.
- Use button to modify group name, VLAN ID, or add/remove the members of the existing VLAN group.

[NOTE] Remember to execute the “Save Configuration” action, otherwise the new configuration will lose when switch power off.

6.17.2 802.1Q VLAN

Tagged-based VLAN is an IEEE 802.1Q specification standard. Therefore, it is possible to create a VLAN across devices from different switch venders. IEEE 802.1Q VLAN uses a technique to insert a “tag” into the Ethernet frames. Tag contains a VLAN Identifier (VID) that indicates the VLAN numbers.
You can create Tag-based VLAN, and enable or disable GVRP protocol. There are 256 VLAN groups to provide configuration. Enable 802.1Q VLAN, all ports on the switch belong to default VLAN of VID 1. The default VLAN can’t be deleted.

GVRP (GARP VLAN Registration Protocol) is a protocol that facilitates control of virtual local area networks (VLANs) within a larger network. GVRP conforms to the IEEE 802.1Q specification, which defines a method of tagging frames with VLAN configuration data. This allows network devices to dynamically exchange VLAN configuration information with other devices.
GVRP is based on GARP (Generic Attribute Registration Protocol), a protocol that defines procedures by which end stations and switches in a local area network (LAN) can register and de-register attributes, such as identifiers or addresses, with each other. Every end station and switch thus has a current record of all the other end stations and switches that can be reached.

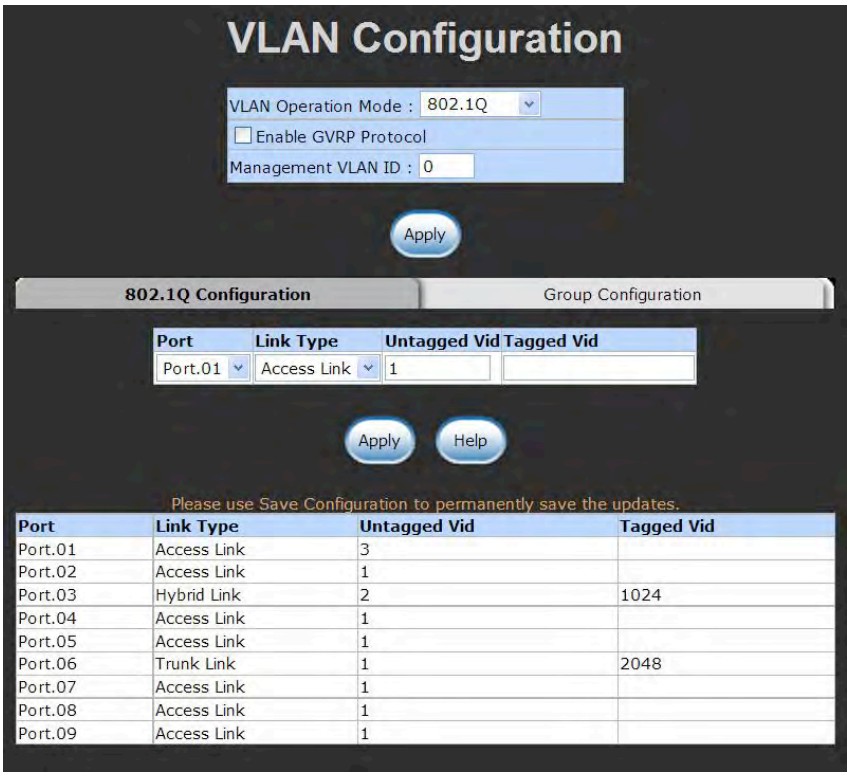
802.1Q Configuration

- Pull down the selection item and focus on **802.1Q** then select the

button to set the VLAN Operation Mode in **802.1Q** mode.
- **Enable GVRP Protocol:** Select the checkbox to enable GVRP protocol. This checkbox is available while the VLAN Operation Mode is in **802.1Q** mode.
- **Management VLAN ID:** The default value is ‘0’ which means VLAN function in 802.1Q mode is not available. While this column field is filled with a value from 1 to 4096, the member ports of this VLAN can access the management interface.

- Select the port you want to configure.
- **Link Type**: There are 3 types of link type.
  - **Access Link:** Single switch only, it allows the user to group ports by assigning the same Untagged VID. While this link type is set, the Untagged VID column field is available but the Tagged VID column field is disabled.
  - **Trunk Link:** The extended application of **Access Link**. It allows the tagged frames go across 2 or more switches by assigning the tagged VID to the frames. Having set this link type, the Tagged VID column field is available but the Untagged VID column field is disabled.
  - **Hybrid Link:** Both **Access Link** and **Trunk Link** are available.
- **Untagged VID:** Assign the untagged frame VID.
- **Tagged VID:** Assign the tagged frame VID.
- Select

button to have the settings taken effect.
- You can see the link type, untagged VID, and tagged VID information of each port in the table below on the screen.



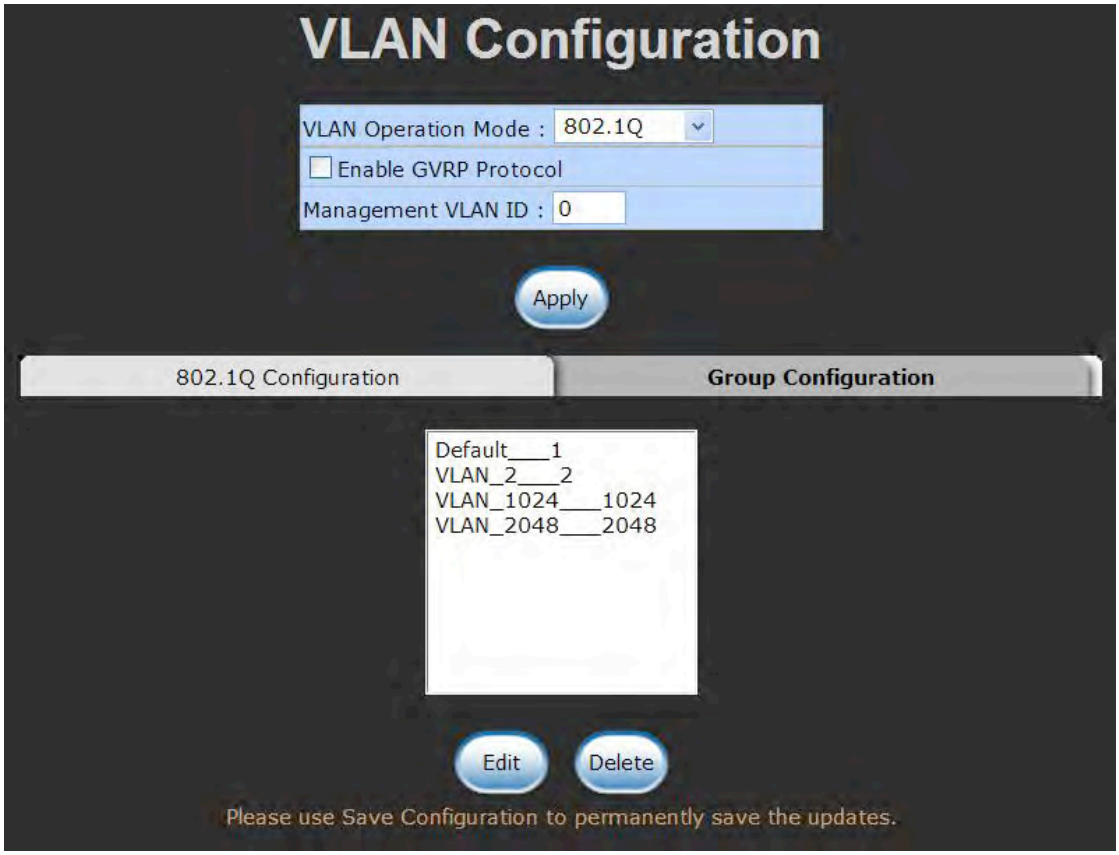
802.1Q VLAN interface

Group Configuration

Edit the existing VLAN Group.

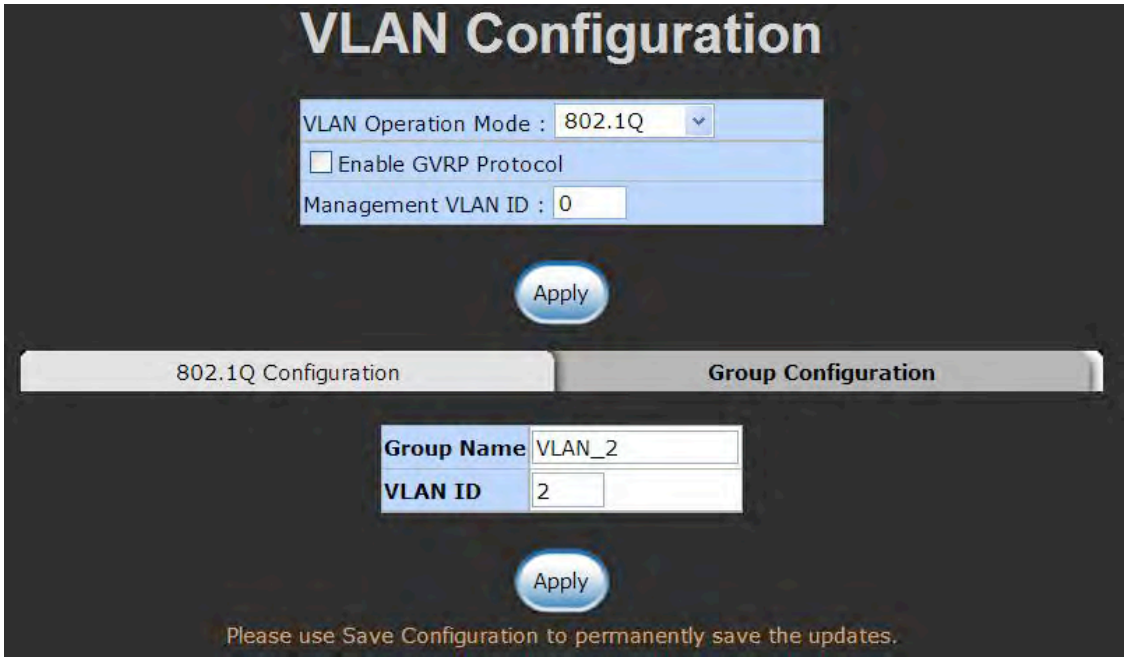
- Select the VLAN group in the table list.
- Select

button.



Group Configuration interface

- You can modify the VLAN group name and VLAN ID.



Group Configuration interface

- Select button.

6.18 Rapid Spanning Tree

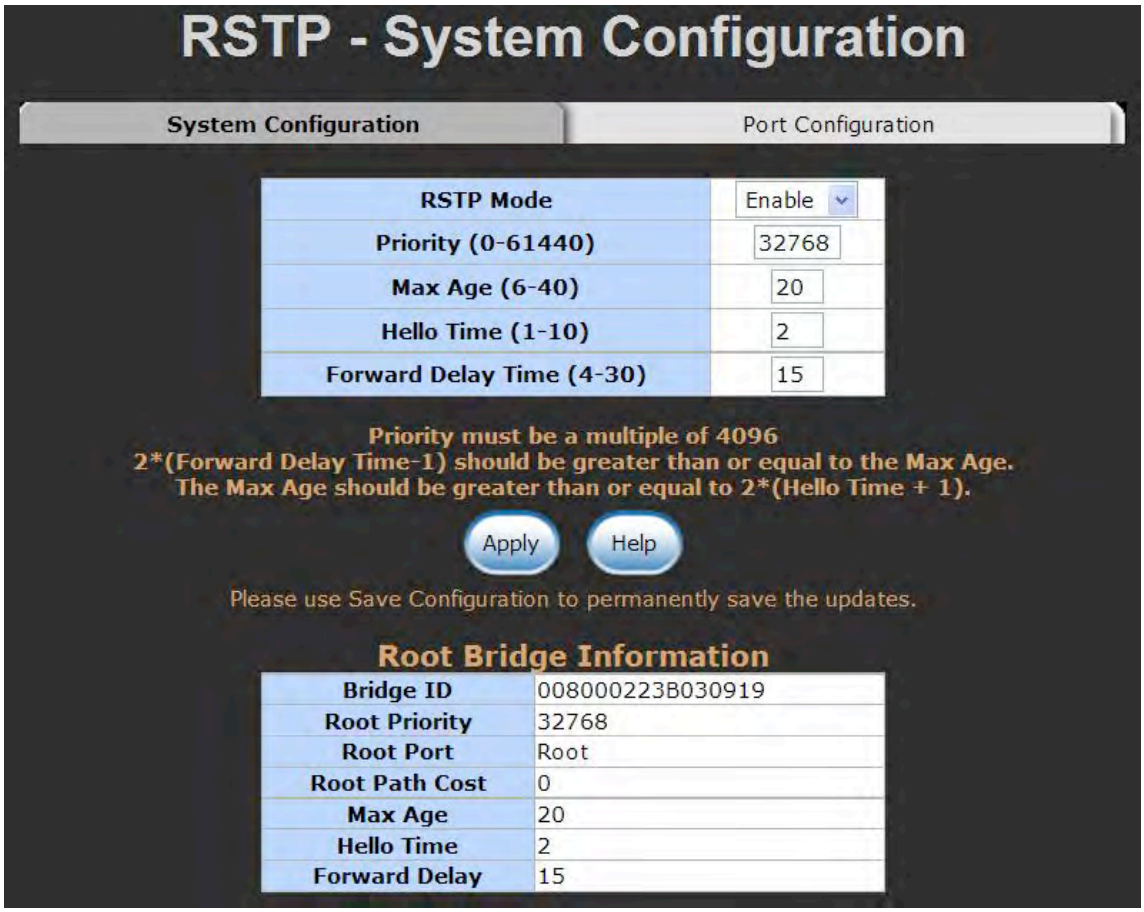
The Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol and provides for faster spanning tree convergence after a topology change. The system also supports STP and the system will auto-detect the connected device that is running STP or RSTP protocol.

6.18.1 RSTP - System Configuration

- The user can view spanning tree information of Root Bridge.
- The user can modify RSTP state. After modification, select

button.
  - **RSTP mode:** The user must enable the RSTP function first before configuring the related parameters.
  - **Priority (0-61440):** The switch with the lowest value has the highest priority and is selected as the root. If the value is changed, the user must reboot the switch. The value must be a multiple of 4096 according to the protocol standard rule.
  - **Max Age (6-40):** The number of seconds a switch waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value between 6 through 40.
  - **Hello Time (1-10):** The time that controls the switch to send out the BPDU packet to check RSTP current status. Enter a value between 1 through 10.
  - **Forward Delay Time (4-30):** The number of seconds a port waits before changing from its Rapid Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a value between 4 through 30.

[NOTE]	Follow the rule as below to configure the MAX Age, Hello Time, and Forward Delay Time. **2 x (Forward Delay Time value –1) > = Max Age value >= 2 x (Hello Time value +1)**



RSTP System Configuration interface

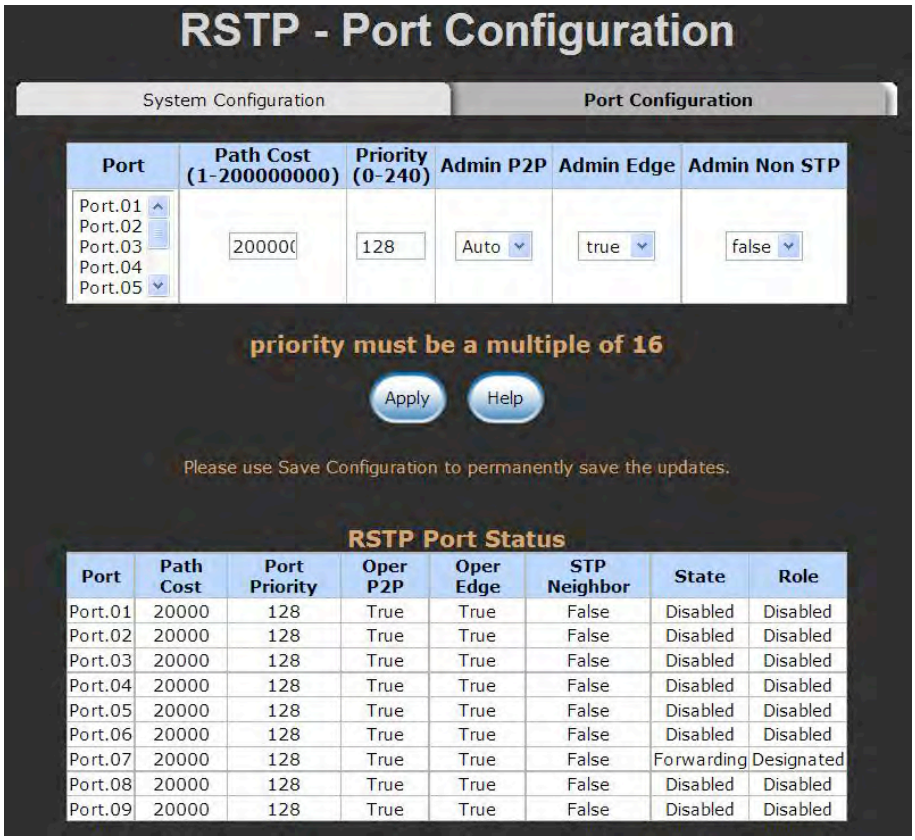
6.18.2 RSTP - Port Configuration

You can configure path cost and priority of every port.

- Select the port in the port column field.
- **Path Cost:** The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200,000,000.
- **Priority:** Decide which port should be blocked by priority in LAN. Enter a number 0

through 240 (the port of the highest value will be blocked). The value of priority must be the multiple of 16.

- **Admin P2P:** Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port concerned can only be connected to exactly one other bridge (i.e. it is served by a point-to-point LAN segment), or can be connected to two or more bridges (i.e. it is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively. True is P2P enabling. False is P2P disabling.
- **Admin Edge:** The port directly connected to end stations won't create bridging loop in the network. To configure the port as an edge port, set the port to "**True**" status.
- **Admin Non STP:** The port includes the STP mathematic calculation. **True** is not including STP mathematic calculation. **False** is including the STP mathematic calculation.
- Select Apply.



RSTP Port Configuration interface

6.19 SNMP Configuration

Simple Network Management Protocol (SNMP) is the protocol developed to manage nodes (servers, workstations, routers, switches and hubs etc.) on an IP network. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Network management systems learn of problems by receiving traps or change notices from network devices implementing SNMP.

6.19.1 System Configuration

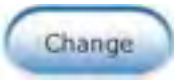
- **Community Strings**

Here you can define the new community string set and remove the unwanted community string.

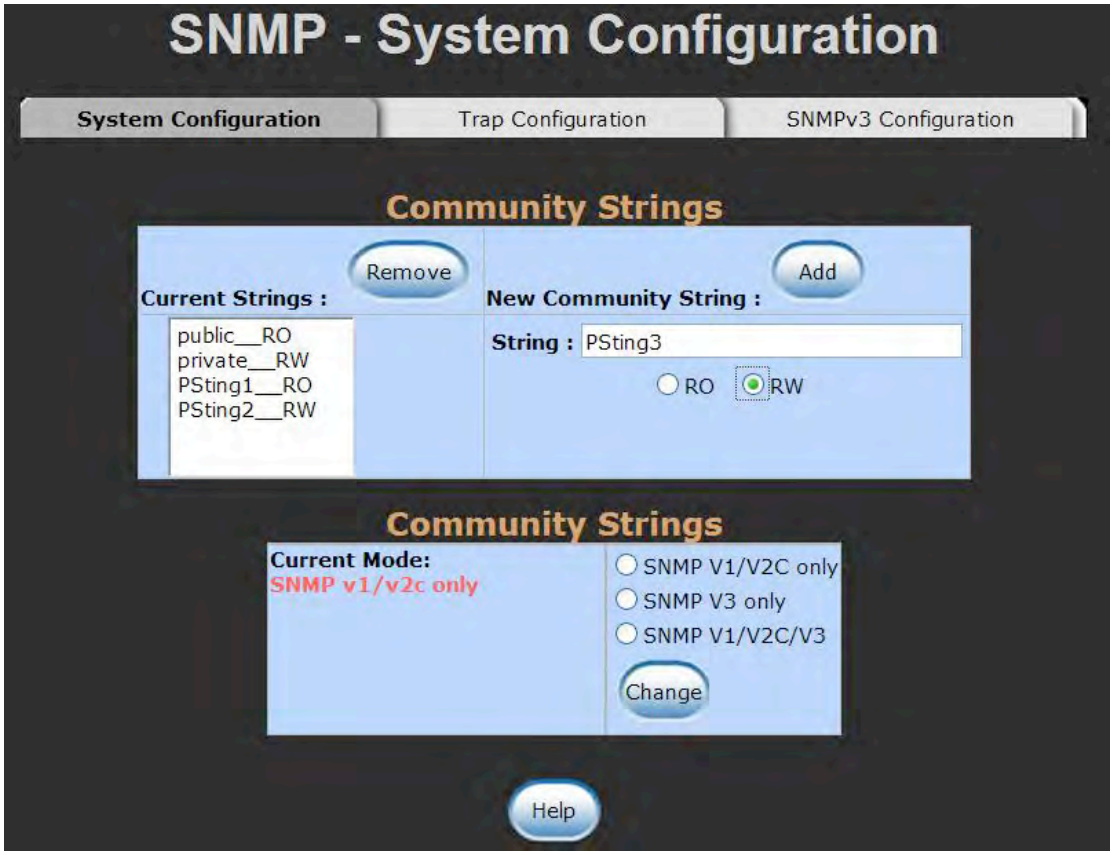
- **String:** Fill the name string.
- **RO:** Read only. Enables requests accompanied by this community string to display MIB-object information.
- **RW:** Read write. Enables requests accompanied by this community string to display MIB-object information and to set MIB objects.
- Select

button.
- To remove the community string, select the community string that you have defined and select

button. You cannot edit the name of the default community string set.

- **Agent Mode:** Select the SNMP version that you want to use and then select 

button to switch to the selected SNMP version mode. The default value is ‘SNMP v1/v2c only’



SNMP System Configuration interface

6.19.2 Trap Configuration

A trap manager is a management station that receives the trap messages generated by the switch. If no trap manager is defined, no traps will be issued. Create a trap manager by entering the IP Address of the station and a community string. To define a management station as a trap manager, assign an IP address, enter the SNMP community strings, and select the SNMP trap version.

- **IP Address:** Enter the IP address of the trap manager.
- **Community:** Enter the community string.
- **Trap Version:** Select the SNMP trap version type—v1 or v2c.
- Select

button.
- To remove the community string, select the community string listed in the current managers field and select

button.

Trap Managers interface

6.19.3 SNMPV3 Configuration

Configure the SNMP V3 function.

Context Table

Configure SNMP v3 context table. Assign the context name of context table. Select

to add context name. Select

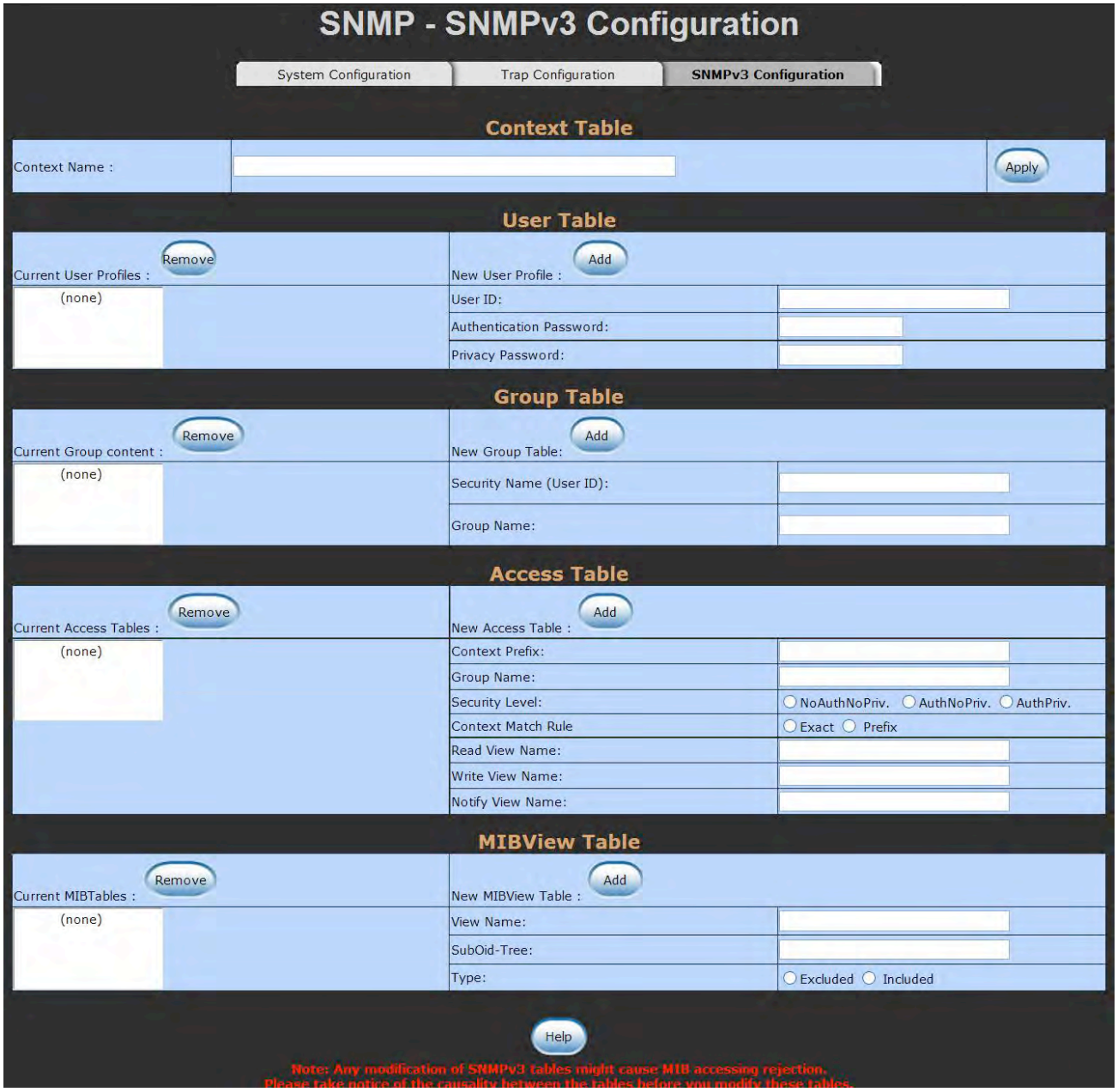
to remove the unwanted context name.

User Profile

Configure SNMP v3 user table..

- **User ID:** Set up the user name.
- **Authentication Password:** Set up the authentication password.
- **Privacy Password:** Set up the private password.

- Select Add to add the context name.
- Select Remove to remove the unwanted context name.



SNMP V3 configuration interface

Group Table

Configure SNMP v3 group table.

- **Security Name (User ID):** Assign the user name that you have set up in user table.
- **Group Name:** Set up the group name.
- Select

to add the group name.
- Select

to remove the unwanted group name.

Access Table

Configure SNMP v3 access table.

- **Context Prefix:** Set up the context name.
- **Group Name:** Set up the group.
- **Security Level:** Set up the access level.
- **Context Match Rule:** Select the context match rule.
- **Read View Name:** Set up the read view.
- **Write View Name:** Set up the write view.
- **Notify View Name:** Set up the notify view.
- Select

to add the context name.
- Select

to remove the unwanted context name.

MIBview Table

Configure MIB view table.

- **ViewName:** Set up the name.
- **Sub-Oid Tree:** Fill the Sub OID.

- **Type:** Select the type—excluded or included.
- Select

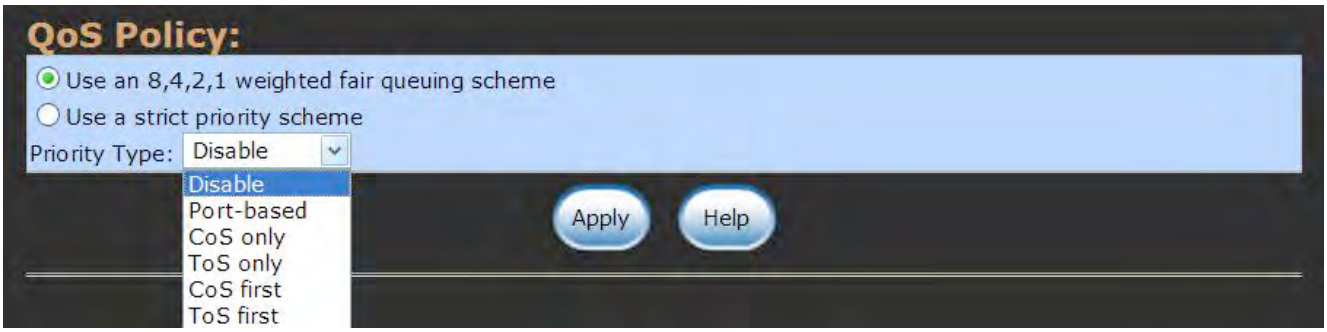
to add the context name.
- Select

to remove the unwanted context name.

6.20 QoS Configuration

Here you can configure QoS policy and priority setting, per port priority setting, COS and TOS setting.

6.20.1 QoS Policy and Priority Type



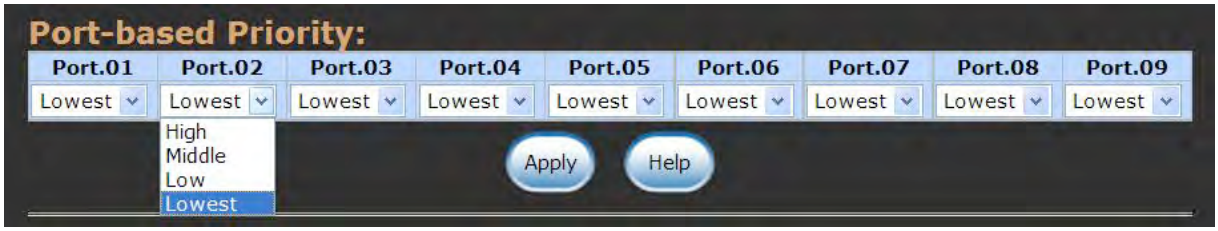
QoS Policy interface

- **QoS Policy:** Select the QoS policy rule.
  - **Using the 8,4,2,1 weight fair queue scheme:** The switch will follow 8:4:2:1 rate to process priority queue from high to lowest queue. For example, while the system is processing, 1 frame of the lowest queue, 2 frames of the low queue, 4 frames of the middle queue, and 8 frames of the high queue will be processed in accordance with the 8,4,2,1 policy rule.
  - **Use a strict priority scheme:** Always the higher queue will be processed first, except the higher queue is empty.
  - **Priority Type:** There are 5 priority type selections available—**Port-based**, **TOS only**, **COS only**, **TOS first**, and **COS first**. Disable means no priority type is selected.
- Select

button to make the settings effective.

6.20.2 Port-based Priority

Configure the priority level for each port. With the drop-down selection item of **Priority Type** above being selected as Port-based, this control item will then be available to set the queuing policy for each port.

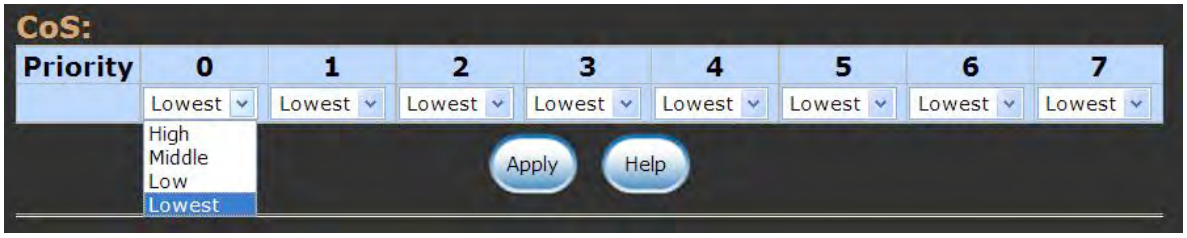


Port-based Priority interface

- **Port x:** Each port has 4 priority levels—High, Middle, Low, and Lowest—to be chosen.
- Select button to make the settings effective.

6.20.3 COS Configuration

Set up the COS priority level. With the drop-down selection item of **Priority Type** above being selected as COS only/COS first, this control item will then be available to set the queuing policy for each port.



COS Configuration interface

- **COS priority:** Set up the COS priority level 0 ~ 7—High, Middle, Low, Lowest.
- Select .

6.20.3 TOS Configuration

Set up the TOS priority. With the drop-down selection item of **Priority Type** above being selected as TOS only/TOS first, this control item will then be available to set the queuing policy for each port.

TOS Configuration interface

■ **TOS priority:** The system provides 0~63 TOS priority level. Each level has 4 types of priority—High, Middle, Low, and Lowest. The default value is 'Lowest' priority for each level. When the IP packet is received, the system will check the TOS level value in the IP packet that has received. For example, the user sets the TOS level 25 as high, the system will check the TOS value of the received IP packet. If the TOS value of received IP packet is 25 (priority = high), and then the packet priority will have highest priority.

■ Select

button to make the settings effective.

6.21 IGMP Configuration

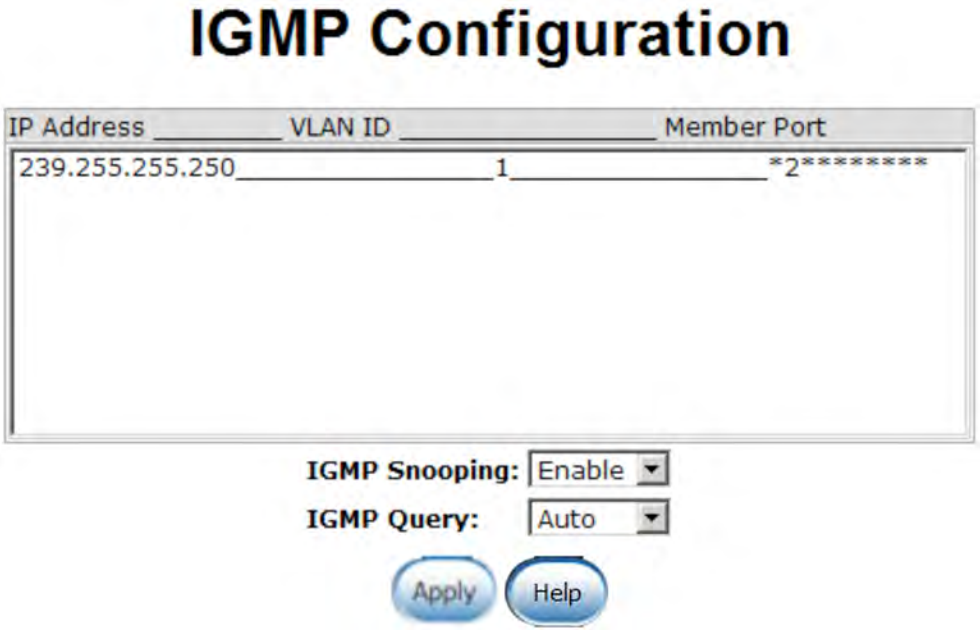
The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, routers, and hosts that support IGMP. Enabling IGMP allows the ports to detect IGMP queries, report packets, and manage IP multicast traffic through the switch. IGMP have three fundamental types of message shown as follows:

Message	Description
Query	A message sent from the querier (IGMP router or switch) asking for a response from each host belonging to the multicast group.
Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host has quit being a member of a specific multicast group.

The switch supports IP multicast. You can enable IGMP protocol via setting the IGMP Configuration page to see the IGMP snooping information. IP multicast addresses are in the range of 224.0.0.0 through 239.255.255.255.

- **IGMP Protocol:** Enable or disable the IGMP protocol.
- **IGMP Query:** Select the IGMP query function as Enable or Auto to set the switch as a querier for IGMP version 2 multicast networks.

- Select Apply button.



IGMP Configuration interface

6.22 X-Ring

X-Ring provides a faster redundant recovery than Spanning Tree topology. The action is similar to STP or RSTP, but the algorithms between them are not the same.

In the X-Ring topology, every switch should be enabled with the X-Ring function and two ports should be assigned as the member ports in the ring. Only one switch in the X-Ring group would be set as the master switch that one of its two member ports would be blocked, called the backup port, and another port is called working port. Other switches in the X-Ring group are called working switches and their two member ports are called working ports. When the failure of a network connection occurs, the backup port of the master switch (Ring Master) will automatically become a working port to recover from the failure.

The switch supports the function and interface for setting the switch as the ringmaster or not. The ringmaster can negotiate and place command to other switches in the X-Ring group. If there are 2 or more switches in master mode, the software will select the switch

with lowest MAC address number as the ringmaster. Setting the X-Ring configuration interface can enable the X-Ring master ring mode.

The system also supports the **Couple Ring** that can connect 2 or more X-Ring group for the redundant backup function; **Dual Homing** function that can prevent connection loss between the X-Ring group and upper level/core switch. Apart from the advantages, **Central Ring** can handle up to 4 rings in the system and has the ability to recover from failure within 300 milliseconds.

- **Enable Ring:** To enable the X-Ring function, select the checkbox beside the **Enable Ring** string label. If this checkbox is not select, all the ring functions are unavailable.
  - **Enable Ring Master:** Select the checkbox to enable this switch to be the ring master.
  - **1st & 2nd Ring Ports:** Pull down the selection menu to assign the ports as the member ports. **1st Ring Port** is the working port and **2nd Ring Port** is the backup port. When **1st Ring Port** fails, the system will automatically upgrade the **2nd Ring Port** to be the working port.
- **Enable Couple Ring:** To enable the coupe ring function, select the checkbox beside the **Enable Couple Ring** string label.
  - **Couple Port:** Assign the member port that is connected to the other ring group.
  - **Control Port:** When the **Enable Couple Ring** checkbox is selected, you have to assign the control port to form a couple-ring group between the two X-rings.
- **Enable Dual Homing:** Set up one of the ports on the switch to be the Dual Homing port. For a switch, there is only one Dual Homing port. Dual Homing function only works when the X-Ring function enabled.
  - **Homing Port:** Assign a port that is used to be the dual homing port.
- And then, select

button to apply the configuration.

X-ring Interface

[NOTE]

1. When the X-Ring function enabled, the user must disable the RSTP. The X-Ring function and RSTP function cannot exist on a switch at the same time.
2. Remember to execute the “Save Configuration” action, otherwise the new configuration will lose when switch powers off.

6.23 LLDP

Link Layer Discovery Protocol (LLDP) is defined in the IEEE 802.1AB, it is an emerging standard which provides a solution for the configuration issues caused by expanding LANs. LLDP specifically defines a standard method for Ethernet network devices such as switches, routers and wireless LAN access points to advertise information about themselves to other nodes on the network and store the information they discover. LLDP runs on all 802 media. The protocol runs over the data-link layer only, allowing two systems running different network layer protocols to learn about each other.

- **LLDP Protocol**: Pull down the selection menu to disable or enable LLDP function.
- **LLDP Interval**: Set the interval of advertising the switch's information to other nodes.
- Click

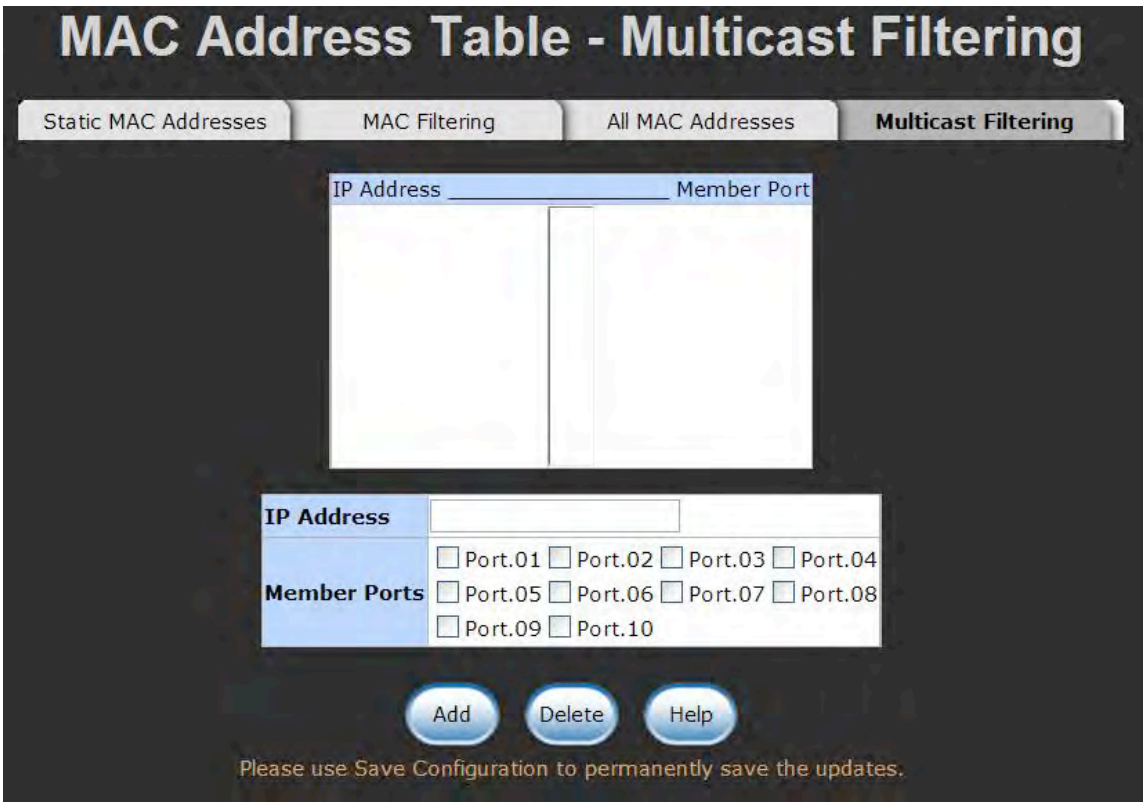
.

LLDP Interface

6.25.4 Multicast Filtering

Multicasts are similar to broadcasts, they are sent to all end stations on a LAN or VLAN. Multicast filtering is the function, which end stations can receive the multicast traffic if the connected ports had been included in the specific multicast groups. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to the registered end stations.

- **IP Address**: Assign a multicast group IP address in the range of 224.0.0.0 ~ 239.255.255.255.
- **Member Ports**: Tick the check box beside the port number to include them as the member ports in the specific multicast group IP address.
- Click Add to append a new filter of multicast to the field, or select the filter in the field and click Delete to remove it.



Multicast Filtering Interface

6.23 Security-802.1X/Radius Configuration

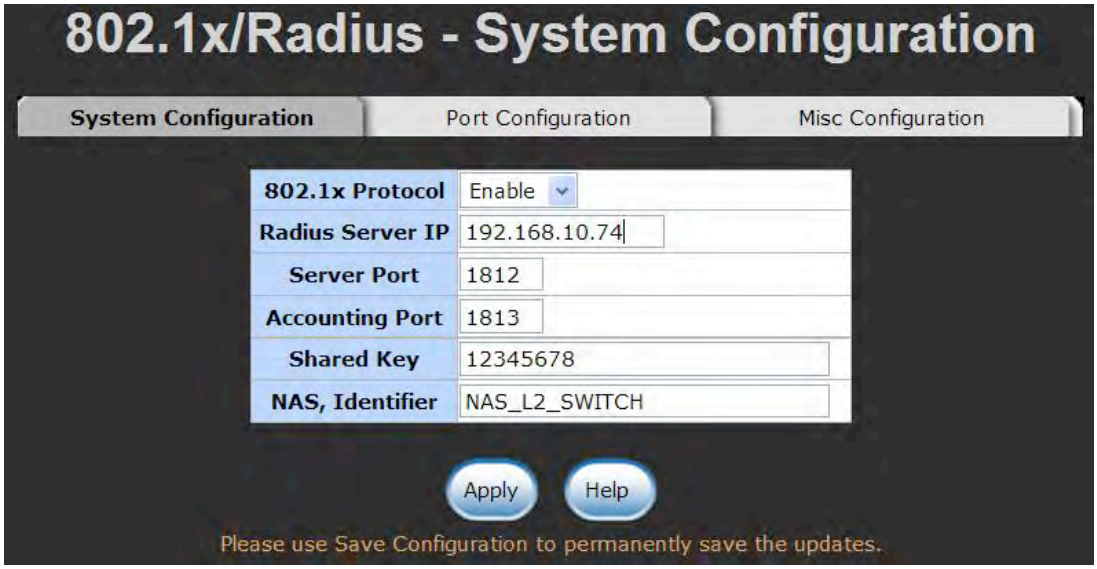
802.1x is an IEEE authentication specification which prevents the client from connecting to a wireless access point or wired switch until it provides authority, like the user name and password that are verified by an authentication server (such as RADIUS server).

6.23.1 System Configuration

After enabling the IEEE 802.1X function, you can configure the parameters of this function.

- **IEEE 802.1x Protocol:** Enable or disable 802.1 x protocols.
- **Radius Server IP:** Assign the RADIUS Server IP address.
- **Server Port:** Set the UDP destination port for authentication requests to the specified RADIUS Server.
- **Accounting Port:** Set the UDP destination port for accounting requests to the specified RADIUS Server.
- **Shared Key:** Set an encryption key for using during authentication sessions with the specified RADIUS server. This key must match the encryption key used on the RADIUS Server.
- **NAS, Identifier:** Set the identifier for the RADIUS client.
- Select

button.

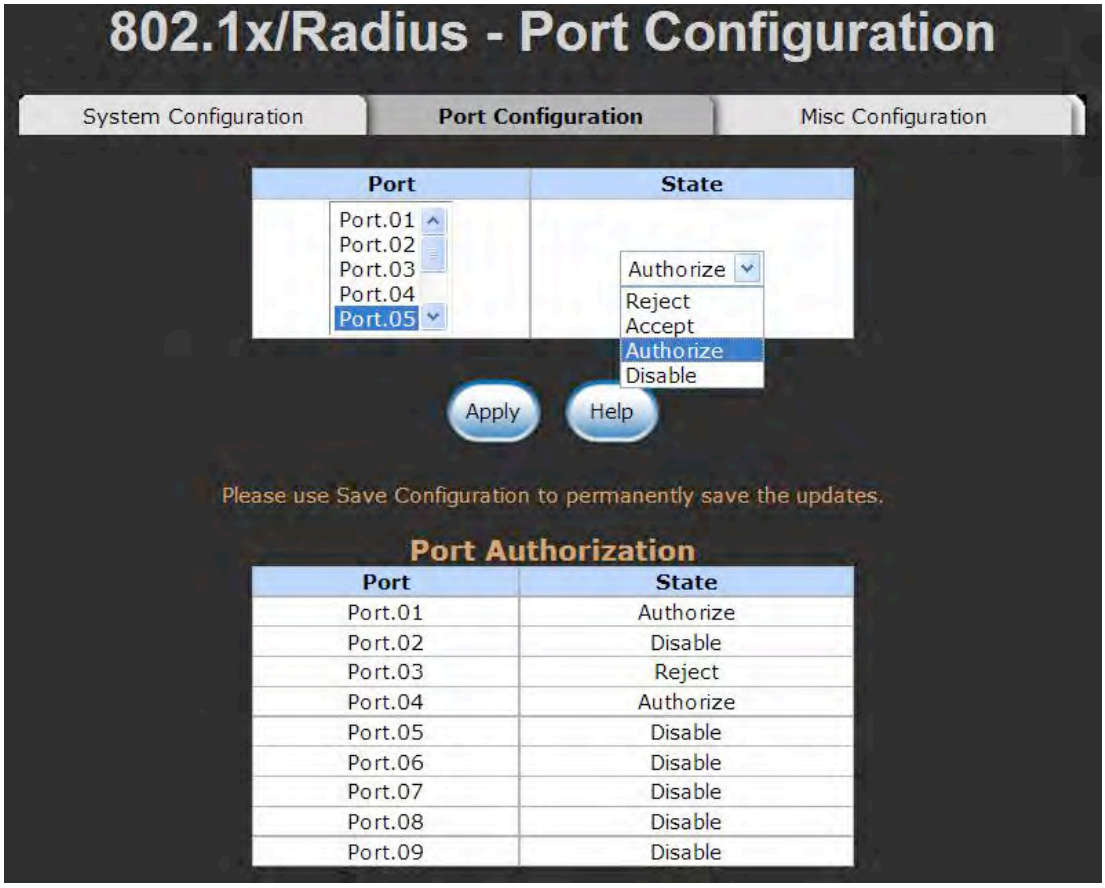


802.1x System Configuration interface

6.23.2 Port Configuration

You can configure the 802.1x authentication state for each port. The state provides Disable, Accept, Reject, and Authorize.

- **Reject:** The specified port is required to be held in the unauthorized state.
- **Accept:** The specified port is required to be held in the authorized state.
- **Authorized:** The specified port is set to the authorized or unauthorized state in accordance with the outcome of an authentication exchange between the Supplicant and the authentication server.
- **Disable:** When disabled, the specified port works without complying with 802.1x protocol.
- Select button.



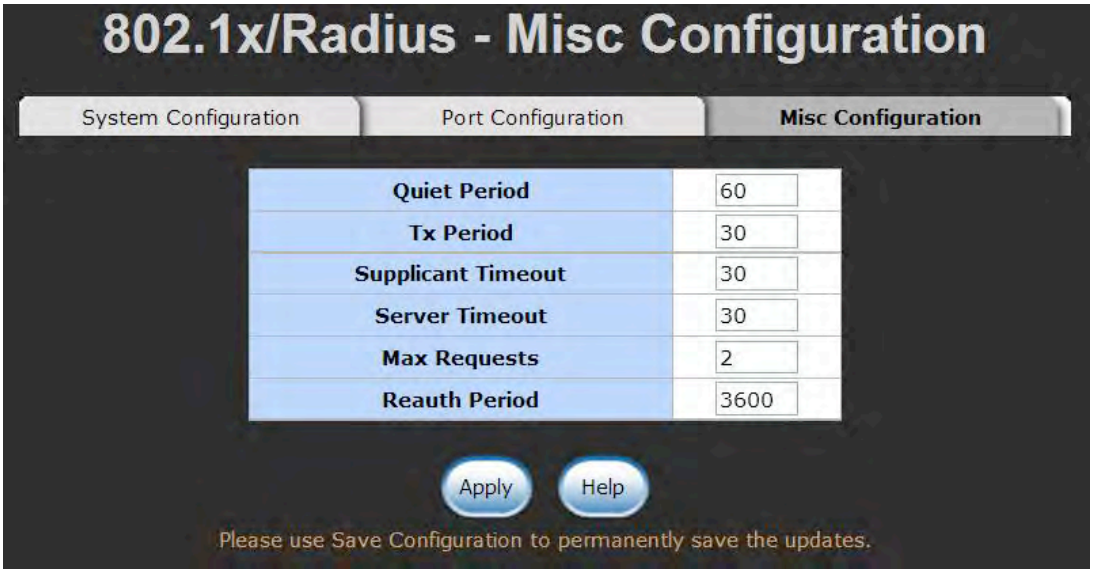
802.1x Per Port Setting interface

6.23.3 Misc Configuration

- **Quiet Period:** Set the period that the port doesn't try to acquire a supplicant.
- **TX Period:** Set the period the port waits for retransmit next EAPOL PDU during an authentication session.
- **Supplicant Timeout:** Set the period of time the switch waits for a supplicant response to an EAP request.
- **Server Timeout:** Set the period of time the switch waits for a server response to an authentication request.
- **Max Requests:** Set the number of authentication that must time-out before authentication fails and the authentication session ends.
- **Reauth period:** Set the period of time that clients connected must be

re-authenticated.

- Select button.



802.1x Misc Configuration interface

6.24 MAC Address Table

Use the MAC address table to ensure the port security.

6.24.1 Static MAC Address

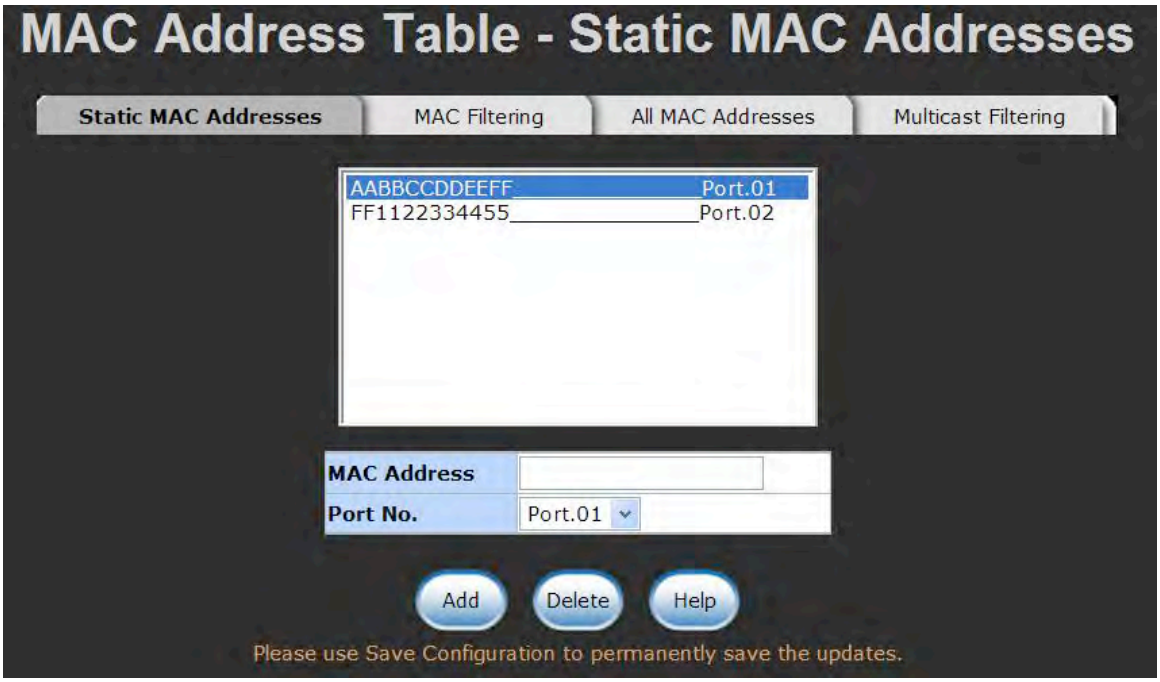
You can add a static MAC address; it remains in the switch's address table, regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when the disconnected or powered-off device is active on the network again. You can add / delete a static MAC address.

Add the Static MAC Address

You can add static MAC addresses in the switch MAC table here.

- **MAC Address:** Enter the MAC address of the port that should permanently forward traffic, regardless of the device network activity.

- **Port No.:** Pull down the selection menu to select the port number.
- Select button.
- If you want to delete the MAC address from filtering table, select the MAC address and select button.



Static MAC Addresses interface

6.24.2 MAC Filtering

By filtering MAC addresses, the switch can easily filter the pre-configured MAC address and reduce the un-safety. You can add and delete filtering MAC address.

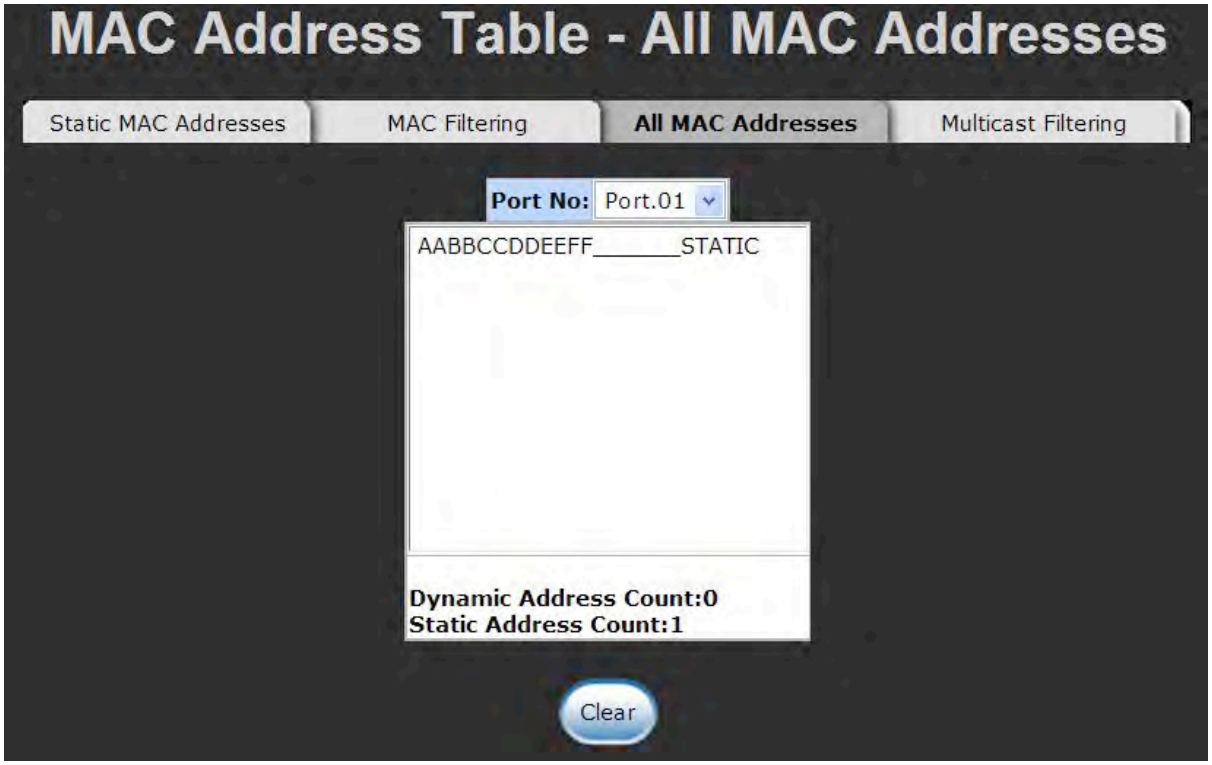
MAC Filtering interface

- **MAC Address:** Enter the MAC address that you want to filter.
- Select button.
- If you want to delete the MAC address from the filtering table, select the MAC address and select button.

6.24.3 All MAC Addresses

You can view the port that connected device's MAC address and the related devices' MAC address.

1. Select the port.
2. The selected port of static & dynamic MAC address information will be displayed in here.
3. Select to clear the current port static MAC address information on screen.



All MAC Address interface

6.25 Factory Default

Reset switch to default configuration. Select

button to reset all configurations to the default value.

Factory Default interface

6.26 Save Configuration

Save all configurations that you have made in the system. To ensure the all configuration

will be saved. Select

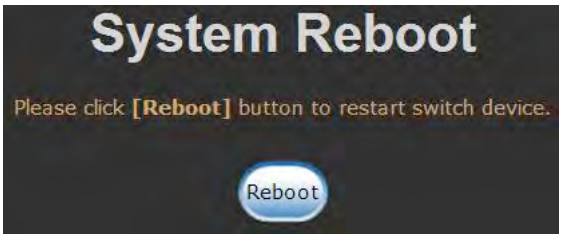
to save the all configuration to the flash memory.

Save Configuration interface

6.27 System Reboot

Reboot the switch in software reset. Select

to reboot the system.



System Reboot interface

Problem Solving

This section is intended to help you solve the most common problems on the CWGE9MS managed Ethernet switch.

Incorrect connections

The switch port can auto detect straight or crossover cable when you link switch with other Ethernet device. For the RJ45 connector should use correct UTP or STP cable, 10/100Mbps port use 2-pairs twisted cable and Gigabit 1000T port use 4 pairs twisted cable. If the RJ45 connector is not the correct pin on right position then the link will fail. For fiber connections, please notice that fiber cable mode and SFP fiber module should match.

Faulty or loose cables

Look for loose or obviously faulty connections. If they appear to be connected, make sure the connections are snug. If that does not correct the problem, substitute a different cable.

Non-standard cables

Non-standard and incorrectly wired cables may cause numerous network collisions and other network problems, and can seriously impair network performance. A category 5-cable tester is a recommended tool for every 100Base-T network installation.

RJ45 ports: use unshielded twisted-pair (UTP) or shielded twisted-pair (STP) cable for RJ45 connections: 100Ω Category 3, 4 or 5 cable for 10Mbps connections or 100Ω Category 5 cable for 100Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet). Gigabit port should use Cat-5 or cat-5e cable for 1000Mbps connections. The length should not exceed 100 meters.

Improper Network Topologies

It is important to make sure that you have a valid network topology. Common topology faults include excessive cable length and too many repeaters (hubs) between end nodes. In addition, you should make sure that your network topology contains no data path loops. Between any two ends nodes, there should be only one active cabling path at any time. Data path loops will cause broadcast storms that will severely impact your network performance.

Diagnostic LED Indicators

The switch can be easily monitored through panel indicators to assist in identifying problems that identify common problems you may encounter and assist in finding possible solutions.

If the power indicator does not turn on when the power cord is plugged in, you may have a problem with power outlet, or power cord. However, if the switch powers off after running for a while check for loose power connections, power losses or surges at power outlet. If you still cannot resolve the problem, contact ComNet for assistance.

Appendix A Command Sets

Commands Set List

User EXEC	**E**
Privileged EXEC	**P**
Global configuration	**G**
VLAN database	**V**
Interface configuration	**I**

System Commands Set

Netstar Commands	Level	Description	Example
show config	**E**	Show switch configuration	switch>**show config**
show terminal	**P**	Show console information	switch#**show terminal**
write memory	**P**	Save user configuration into permanent memory (flash rom)	switch#**write memory**
system name [System Name]	**G**	Configure system name	switch(config)#**system name xxx**
system location [System Location]	**G**	Set switch system location string	switch(config)#**system location xxx**
system description [System Description]	**G**	Set switch system description string	switch(config)#**system description xxx**
system contact [System Contact]	**G**	Set switch system contact window string	switch(config)#**system contact xxx**
show system-info	**E**	Show system information	switch>**show system-info**

ip address **[Ip-address]** **[Subnet-mask]** **[Gateway]**	**G**	Configure the IP address of switch	switch(config)**#ip address 192.168.1.1 255.255.255.0 192.168.1.254**
ip dhcp	**G**	Enable DHCP client function of switch	switch(config)**#ip dhcp**
show ip	**P**	Show IP information of switch	switch**#show ip**
no ip dhcp	**G**	Disable DHCP client function of switch	switch(config)**#no ip dhcp**
reload	**G**	Halt and perform a cold restart	switch(config)**#reload**
default	**G**	Restore to default	switch(config)**#default**
admin username **[Username]**	**G**	Changes a login username. (maximum 10 words)	switch(config)**#admin username xxxxxx**
admin password **[Password]**	**G**	Specifies a password (maximum 10 words)	switch(config)**#admin password xxxxxx**
show admin	**P**	Show administrator information	switch**#show admin**
dhcpserver enable	**G**	Enable DHCP Server	switch(config)**#dhcpserver enable**
dhcpserver disable	**G**	Disable DHCP Server	switch(config)**#no dhcpserver**
dhcpserver lowip **[Low IP]**	**G**	Configure low IP address for IP pool	switch(config)**#dhcpserver lowip 192.168.1.100**
dhcpserver highip **[High IP]**	**G**	Configure high IP address for IP pool	switch(config)**#dhcpserver highip 192.168.1.200**
dhcpserver subnetmask **[Subnet mask]**	**G**	Configure subnet mask for DHCP clients	switch(config)**#dhcpserver subnetmask 255.255.255.0**
dhcpserver gateway **[Gateway]**	**G**	Configure gateway for DHCP clients	switch(config)**#dhcpserver gateway 192.168.1.254**

dhcpserver dnsip [DNS IP]	**G**	Configure DNS IP for DHCP clients	switch(config)#**dhcpserver dnsip 192.168.1.1**
dhcpserver leasetime [SEC.]	**G**	Configure lease time (in sec.)	switch(config)#**dhcpserver leasetime 86400**
dhcpserver ipbinding [IP address]	**I**	Set static IP for DHCP clients by port	switch(config)#**interface fastEthernet 2** switch(config)#**dhcpserver ipbinding 192.168.1.1**
show dhcpserver configuration	**P**	Show configuration of DHCP server	switch#**show dhcpserver configuration**
show dhcpserver clients	**P**	Show client entries of DHCP server	switch#**show dhcpserver clients**
show dhcpserver ip-binding	**P**	Show IP-Binding information of DHCP server	switch#**show dhcpserver ip-binding**
no dhcpserver	**G**	Disable DHCP server function	switch(config)#**no dhcpserver**
security enable	**G**	Enable IP security function	switch(config)#**security enable**
security http	**G**	Enable IP security of HTTP server	switch(config)#**security http**
security telnet	**G**	Enable IP security of telnet server	switch(config)#**security telnet**
security ip [Index(1..10)] [IP Address]	**G**	Set the IP security list	switch(config)#**security ip 1 192.168.1.55**
show security	**P**	Show the information of IP security	switch#**show security**
no security	**G**	Disable IP security function	switch(config)#**no security**

no security http	**G**	Disable IP security of HTTP server	switch(config)**#no security http**
no security telnet	**G**	Disable IP security of telnet server	switch(config)**#no security telnet**

Port Commands Set

Netstar Commands	Level	Description	Example
interface fastEthernet **[Portid]**	**G**	Choose the port for modification.	switch(config)**#interface fastEthernet 2**
duplex **[full | half]**	**I**	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	switch(config)**#interface fastEthernet 2** switch(config-if)**#duplex full**
speed **[10|100|1000|auto]**	**I**	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet., the speed can't be set to 1000 if the port isn't a giga port..	switch(config)**#interface fastEthernet 2** switch(config-if)**#speed 100**
flowcontrol enable **[enable|disable]**	**I**	Configure flow control	switch(config-if)**#flowcontrol enable**
no flowcontrol	**I**	Disable flow control of interface	switch(config-if)**#no flowcontrol**

security enable	**I**	Enable security of interface	switch(config)**#interface fastEthernet 2** switch(config-if)**#security enable**
no security	**I**	Disable security of interface	switch(config)**#interface fastEthernet 2** switch(config-if)**#no security**
bandwidth type all	**I**	Set interface ingress limit frame type to “accept all frame”	switch(config)**#interface fastEthernet 2** switch(config-if)**#bandwidth type all**
bandwidth type broadcast-multicast-flooded-unicast	**I**	Set interface ingress limit frame type to “accept broadcast, multicast, and flooded unicast frame”	switch(config)**#interface fastEthernet 2** switch(config-if)**#bandwidth type broadcast-multicast-flooded-unicast**
bandwidth type broadcast-multicast	**I**	Set interface ingress limit frame type to “accept broadcast and multicast frame”	switch(config)**#interface fastEthernet 2** switch(config-if)**#bandwidth type broadcast-multicast**
bandwidth type broadcast-only	**I**	Set interface ingress limit frame type to “only accept broadcast frame”	switch(config)**#interface fastEthernet 2** switch(config-if)**#bandwidth type broadcast-only**
bandwidth in **[Value]**	**I**	Set interface input bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config)**#interface fastEthernet 2** switch(config-if)**#bandwidth in 100**

bandwidth out [Value]		Set interface output bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config)**#interface fastEthernet 2** switch(config-if)**#bandwidth out 100**
show bandwidth	**I**	Show interfaces bandwidth control	switch(config)**#interface fastEthernet 2** switch(config-if)**#show bandwidth**
state [Enable | Disable]	**I**	Use the state interface configuration command to specify the state mode of operation for Ethernet ports. Use the disable form of this command to disable the port.	switch(config)**#interface fastEthernet 2** (config-if)**#state Disable**
show interface configuration	**I**	show interface configuration status	switch(config)**#interface fastEthernet 2** switch(config-if)**#show interface configuration**
show interface status	**I**	show interface actual status	switch(config)**#interface fastEthernet 2** (config-if)**#show interface status**
show interface accounting	**I**	show interface statistic counter	switch(config)**#interface fastEthernet 2** (config-if)**#show interface accounting**
no accounting	**I**	Clear interface accounting information	switch(config)**#interface fastEthernet 2** switch(config-if)**#no accounting**

Trunk Commands Set

Netstar Commands	Level	Description	Example
aggregator priority [1~65535]	G	Set port group system priority	switch(config)#**aggregator priority 22**
aggregator activityport [Group ID] [Port Numbers]	G	Set activity port	switch(config)#**aggregator activityport 2 2**
aggregator group [GroupID] [Port-list] **lacp** **workp** [Workport]	G	Assign a trunk group with LACP active. [GroupID] :1~3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6) [Workport]: The amount of work ports, this value could not be less than zero or be large than the amount of member ports.	switch(config)#**aggregator group 1 1-4 lacp workp 2** or switch(config)#**aggregator group 2 1,4,3 lacp workp 3**
aggregator group [GroupID] [Port-list] **nolacp**	G	Assign a static trunk group. [GroupID] :1~3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6)	switch(config)#**aggregator group 1 2-4 nolacp** or switch(config)#**aggregator group 1 3,1,2 nolacp**

show aggregator [Group-number]	**P**	Show the information of trunk group	switch#**show aggregator 1** or switch#**show aggregator 2** or switch#**show aggregator 3**
no aggregator lacp [GroupID]	**G**	Disable the LACP function of trunk group	switch(config)#**no aggreator lacp 1**
no aggregator group [GroupID]	**G**	Remove a trunk group	switch(config)#**no aggreator group 2**

VLAN Commands Set

Netstar Commands	Level	Description	Example
vlan database	**P**	Enter VLAN configure mode	switch#**vlan database**
Vlanmode [portbase| 802.1q | gvrp]	**V**	To set switch VLAN mode.	switch(vlan)#**vlanmode portbase** or switch(vlan)#**vlanmode 802.1q** or switch(vlan)#**vlanmode gvrp**
no vlan	**V**	No VLAN	Switch(vlan)#**no vlan**
Ported based VLAN configuration			
vlan port-based grpname [Group Name] **grpid** [GroupID] **port** [PortNumbers]	**V**	Add new port based VALN	switch(vlan)#**vlan port-based grpname test grpid 2 port 2-4** or switch(vlan)#**vlan port-based grpname test grpid 2 port 2,3,4**
show vlan [GroupID] or **show vlan**	**V**	Show VLAN information	switch(vlan)#**show vlan 23**

no vlan group [GroupID]	**V**	Delete port base group ID	switch(vlan)**#no vlan group 2**
IEEE 802.1Q VLAN			
vlan 8021q name [GroupName] **vid** [VID]	**V**	Change the name of VLAN group, if the group didn't exist, this command can't be applied.	switch(vlan)**#vlan 8021q name test vid 22**
vlan 8021q port [PortNumber] **access-link untag** [UntaggedVID]	**V**	Assign a access link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)**#vlan 8021q port 3 access-link untag 33**
vlan 8021q port [PortNumber] **trunk-link tag** [TaggedVID List]	**V**	Assign a trunk link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)**#vlan 8021q port 3 trunk-link tag 2,3,6,99** or switch(vlan)**#vlan 8021q port 3 trunk-link tag 3-20**
vlan 8021q port [PortNumber] **hybrid-link untag** [UntaggedVID] **tag** [TaggedVID List]	**V**	Assign a hybrid link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)**#vlan 8021q port 3 hybrid-link untag 4 tag 3,6,8** or switch(vlan)**#vlan 8021q port 3 hybrid-link untag 5 tag 6-8**
vlan 8021q trunk [PortNumber] **access-link untag** [UntaggedVID]	**V**	Assign a access link for VLAN by trunk group	switch(vlan)**#vlan 8021q trunk 3 access-link untag 33**

vlan 8021q trunk **[PortNumber]** **trunk-link tag** **[TaggedVID List]**	**V**	Assign a trunk link for VLAN by trunk group	switch(vlan)**#vlan 8021q trunk 3 trunk-link tag 2,3,6,99** or switch(vlan)**#vlan 8021q trunk 3 trunk-link tag 3-20**
vlan 8021q trunk **[PortNumber]** **hybrid-link untag** **[UntaggedVID]** **tag** **[TaggedVID List]**	**V**	Assign a hybrid link for VLAN by trunk group	switch(vlan)**#vlan 8021q trunk 3 hybrid-link untag 4 tag 3,6,8** or switch(vlan)**#vlan 8021q trunk 3 hybrid-link untag 5 tag 6-8**

Spanning Tree Commands Set

Netstar Commands	Level	Description	Example
spanning-tree enable	**G**	Enable spanning tree	switch(config)**#spanning-tree enable**
spanning-tree priority [0~61440]	**G**	Configure spanning tree priority parameter	switch(config)**#spanning-tree priority 32767**
spanning-tree max-age [seconds]	**G**	Use the spanning-tree max-age global configuration command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputed the Spanning Tree Protocol (STP) topology.	switch(config)**#spanning-tree max-age 15**
spanning-tree hello-time [seconds]	**G**	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs).	switch(config)**#spanning-tree hello-time 3**

spanning-tree forward-time [seconds]	**G**	Use the spanning-tree forward-time global configuration command to set the forwarding-time for the specified spanning-tree instances. The forwarding time determines how long each of the listening and learning states last before the port begins forwarding.	switch(config)#**spanning-tree forward-time 20**
stp-path-cost [1~200000000]	**I**	Use the spanning-tree cost interface configuration command to set the path cost for Spanning Tree Protocol (STP) calculations. In the event of a loop, spanning tree considers the path cost when selecting an interface to place into the forwarding state.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-path-cost 20**

stp-path-priority [Port Priority]	**I**	Use the spanning-tree port-priority interface configuration command to configure a port priority that is used when two switches tie for position as the root switch.	switch(config)**#interface fastEthernet 2** switch(config-if)**#stp-path-priority 128**
stp-admin-p2p [Auto|True|False]	**I**	Admin P2P of STP priority on this interface.	switch(config)**#interface fastEthernet 2** switch(config-if)**#stp-admin-p2p Auto**
stp-admin-edge [True|False]	**I**	Admin Edge of STP priority on this interface.	switch(config)**#interface fastEthernet 2** switch(config-if)**#stp-admin-edge True**
stp-admin-non-stp [True|False]	**I**	Admin NonSTP of STP priority on this interface.	switch(config)**#interface fastEthernet 2** switch(config-if)**#stp-admin-non-stp False**
show spanning-tree	**E**	Displays a summary of the spanning-tree states.	switch>**show spanning-tree**
no spanning-tree	**G**	Disable spanning-tree.	switch(config)**#no spanning-tree**

QOS Commands Set

Netstar Commands	Level	Description	Example
qos policy [weighted-fair|strict]	G	Select QOS policy scheduling	switch(config)#**qos policy weighted-fair**
qos prioritytype [port-based|cos-only|tos-only|cos-first|tos-first]	G	Setting of QOS priority type	switch(config)#**qos prioritytype**
qos priority portbased [Port] [lowest|low|middle|high]	G	Configure Port-based Priority	switch(config)#**qos priority portbased 1 low**
qos priority cos [Priority][lowest|low|middle|high]	G	Configure COS Priority	switch(config)#**qos priority cos 0 middle**
qos priority tos [Priority][lowest|low|middle|high]	G	Configure TOS Priority	switch(config)#**qos priority tos 3 high**
show qos	P	Displays the information of QoS configuration	Switch#**show qos**
no qos	G	Disable QoS function	switch(config)#**no qos**

IGMP Commands Set

Netstar Commands	Level	Description	Example
igmp enable	**G**	Enable IGMP snooping function	switch(config)#**igmp enable**
lgmp-query auto	**G**	Set IGMP query to auto mode	switch(config)#**lgmp-query auto**
lgmp-query force	**G**	Set IGMP query to force mode	switch(config)#**lgmp-query force**
show igmp configuration	**P**	Displays the details of an IGMP configuration.	switch#**show igmp configuration**
show igmp multi	**P**	Displays the details of an IGMP snooping entries.	switch#**show igmp multi**
no igmp	**G**	Disable IGMP snooping function	switch(config)#**no igmp**
no igmp-query	**G**	Disable IGMP query	switch#**no igmp-query**

Mac / Filter Table Commands Set

Netstar Commands	Level	Description	Example
mac-address-table static hwaddr [MAC]	I	Configure MAC address table of interface (static).	switch(config)#**interface fastEthernet 2** switch(config-if)#**mac-address-table static hwaddr 000012345678**
mac-address-table filter hwaddr [MAC]	G	Configure MAC address table(filter)	switch(config)#**mac-address-table filter hwaddr 000012348678**
show mac-address-table	P	Show all MAC address table	switch#**show mac-address-table**
show mac-address-table static	P	Show static MAC address table	switch#**show mac-address-table static**
show mac-address-table filter	P	Show filter MAC address table.	switch#**show mac-address-table filter**
no mac-address-table static hwaddr [MAC]	I	Remove an entry of MAC address table of interface (static)	switch(config)#**interface fastEthernet 2** switch(config-if)#**no mac-address-table static hwaddr 000012345678**
no mac-address-table filter hwaddr [MAC]	G	Remove an entry of MAC address table (filter)	switch(config)#**no mac-address-table filter hwaddr 000012348678**
no mac-address-table	G	Remove dynamic entry of MAC address table	switch(config)#**no mac-address-table**

SNMP Commands Set

Netstar Commands	Level	Description	Example
snmp system-name [System Name]	G	Set SNMP agent system name	switch(config)#**snmp system-name l2switch**
snmp system-location [System Location]	G	Set SNMP agent system location	switch(config)#**snmp system-location lab**
snmp system-contact [System Contact]	G	Set SNMP agent system contact	switch(config)#**snmp system-contact where**
snmp agent-mode [v1v2c|v3|v1v2cv3]	G	Select the agent mode of SNMP	switch(config)#**snmp agent-mode v1v2cv3**
snmp community-strings [Community] **right** [RO/RW]	G	Add SNMP community string.	switch(config)#**snmp community-strings public right rw**
snmp-server host [IP address] **community** [Community-string] **trap-version** [v1|v2c]	G	Configure SNMP server host information and community string	switch(config)#**snmp-server host 192.168.1.50 community public trap-version v1 (remove)** Switch(config)#**no snmp-server host 192.168.1.50**
snmpv3 context-name [Context Name]	G	Configure the context name	switch(config)#**snmpv3 context-name Test**
snmpv3 user [User Name] **group** [Group Name] **password** [Authentication Password] [Privacy Password]	G	Configure the user profile for SNMPV3 agent. Privacy password could be empty.	switch(config)#**snmpv3 user test01 group G1 password AuthPW PrivPW**

snmpv3 access context-name [Context Name] **group** [Group Name] **security-level** [NoAuthNoPriv|AuthNoPriv|AuthPriv] **match-rule** [Exact|Prifix] **views** [Read View Name] [Write View Name] [Notify View Name]	**G**	Configure the access table of SNMPV3 agent	switch(config)**#snmpv3 access context-name Test group G1 security-level AuthPriv match-rule Exact views V1 V1 V1**
snmpv3 mibview view [View Name] **type** [Excluded|Included] **sub-oid** [OID]	**G**	Configure the mibview table of SNMPV3 agent	switch(config)**#snmpv3 mibview view V1 type Excluded sub-oid 1.3.6.1**
show snmp	**P**	Show SNMP configuration	switch**#show snmp**
no snmp community-strings [Community]	**G**	Remove the specified community.	switch(config)**#no snmp community-strings public**
no snmp-server host [Host-address]	**G**	Remove the SNMP server host.	switch(config)**#no snmp-server 192.168.1.50**
no snmpv3 user [User Name]	**G**	Remove specified user of SNMPv3 agent.	switch(config)**#no snmpv3 user Test**

no snmpv3 access context-name [Context Name] **group** [Group Name] **security-level** [NoAuthNoPriv|AuthNoPriv|AuthPriv] **match-rule** [Exact|Prifix] **views** [Read View Name] [Write View Name] [Notify View Name]	**G**	Remove specified access table of SNMPv3 agent.	switch(config)**#no snmpv3 access context-name Test group G1 security-level AuthPriv match-rule Exact views V1 V1 V1**
no snmpv3 mibview view [View Name] **type** [Excluded|Included] **sub-oid** [OID]	**G**	Remove specified mibview table of SNMPV3 agent.	switch(config)**#no snmpv3 mibview view V1 type Excluded sub-oid 1.3.6.1**

Port Mirroring Commands Set

Netstar Commands	Level	Description	Example
monitor rx	**G**	Set RX destination port of monitor function	switch(config)**#monitor rx**
monitor tx	**G**	Set TX destination port of monitor function	switch(config)**#monitor tx**
show monitor	**P**	Show port monitor information	switch**#show monitor**
monitor [RX|TX|Both]	**I**	Configure source port of monitor function	switch(config)**#interface fastEthernet 2** switch(config-if)**#monitor RX**
show monitor	**I**	Show port monitor information	switch(config)**#interface fastEthernet 2** switch(config-if)**#show monitor**
no monitor	**I**	Disable source port of monitor function	switch(config)**#interface fastEthernet 2** switch(config-if)**#no monitor**

802.1x Commands Set

Netstar Commands	Level	Description	Example
8021x enable	**G**	Use the 802.1x global configuration command to enable 802.1x protocols.	switch(config)# **8021x enable**
8021x system radiusip [IP address]	**G**	Use the 802.1x system radius IP global configuration command to change the radius server IP.	switch(config)# **8021x system radiusip 192.168.1.1**
8021x system serverport [port ID]	**G**	Use the 802.1x system server port global configuration command to change the radius server port	switch(config)# **8021x system serverport 1815**
8021x system accountport [port ID]	**G**	Use the 802.1x system account port global configuration command to change the accounting port	switch(config)# **8021x system accountport 1816**
8021x system sharekey [SharedKey]	**G**	Use the 802.1x system share key global configuration command to change the shared key value.	switch(config)# **8021x system sharekey 123456**

8021x system nasid [NAS ID]	**G**	Use the 802.1x system nasid global configuration command to change the NAS ID	switch(config)# **8021x system nasid test1**
8021x misc quietperiod [sec.]	**G**	Use the 802.1x misc quiet period global configuration command to specify the quiet period value of the switch.	switch(config)# **8021x misc quietperiod 10**
8021x misc txperiod [sec.]	**G**	Use the 802.1x misc TX period global configuration command to set the TX period.	switch(config)# **8021x misc txperiod 5**
8021x misc supportimeout [sec.]	**G**	Use the 802.1x misc supp timeout global configuration command to set the supplicant timeout.	switch(config)# **8021x misc supportimeout 20**
8021x misc servertimeout [sec.]	**G**	Use the 802.1x misc server timeout global configuration command to set the server timeout.	switch(config)#**8021x misc servertimeout 20**

8021x misc maxrequest [number]	**G**	Use the 802.1x misc max request global configuration command to set the MAX requests.	switch(config)# **8021x misc maxrequest 3**
8021x misc reauthperiod [sec.]	**G**	Use the 802.1x misc reauth period global configuration command to set the reauth period.	switch(config)# **8021x misc reauthperiod 3000**
8021x portstate [disable | reject | accept | authorize]	**I**	Use the 802.1x port state interface configuration command to set the state of the selected port.	switch(config)#**interface fastethernet 3** switch(config-if)#**8021x portstate accept**
show 8021x	**E**	Displays a summary of the 802.1x properties and also the port sates.	switch>**show 8021x**
no 8021x	**G**	Disable 802.1x function	switch(config)#**no 8021x**

TFTP Commands Set

Netstar Commands	Level	Description	Defaults Example
backup flash:backup_cfg	**G**	Save configuration to TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)**#backup flash:backup_cfg**
restore flash:restore_cfg	**G**	Get configuration from TFTP server and need to specify the IP of TFTP server and the file name of image.	switch(config)**#restore flash:restore_cfg**
upgrade flash:upgrade_fw	**G**	Upgrade firmware by TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)**#upgrade lash:upgrade_fw**

SystemLog, SMTP and Event Commands Set

Netstar Commands	Level	Description	Example
systemlog ip [IP address]	**G**	Set System log server IP address.	switch(config)# **systemlog ip 192.168.1.100**
systemlog mode [client|server|both]	**G**	Specified the log mode	switch(config)# **systemlog mode both**
show systemlog	**E**	Displays system log.	Switch>**show systemlog**
show systemlog	**P**	Show system log client & server information	switch**#show systemlog**
no systemlog	**G**	Disable systemlog functon	switch(config)**#no systemlog**

smtp enable	**G**	Enable SMTP function	switch(config)**#smtp enable**
smtp serverip [IP address]	**G**	Configure SMTP server IP	switch(config)**#smtp serverip 192.168.1.5**
smtp sender [sendername]	**G**	Configure sender of mail	switch(config)**#smtp sender dut1@xxx.com**
smtp authentication	**G**	Enable SMTP authentication	switch(config)**#smtp authentication**
smtp account [account]	**G**	Configure authentication account	switch(config)**#smtp account John**
smtp password [password]	**G**	Configure authentication password	switch(config)**#smtp password 1234**
smtp rcptemail [Index] [Email address]	**G**	Configure Rcpt e-mail Address	switch(config)**#smtp rcptemail 1** Alert@test.com
show smtp	**P**	Show the information of SMTP	switch**#show smtp**
no smtp	**G**	Disable SMTP function	switch(config)**#no smtp**
event device-cold-start [Systemlog|SMTP|Both]	**G**	Set cold start event type	switch(config)**#event device-cold-start both**
event device-warm-start [Systemlog|SMTP|Both]	**G**	Set warm start event type	switch(config)**#event device-warm-start both**
event authentication-failure [Systemlog|SMTP|Both]	**G**	Set Authentication failure event type	switch(config)**#event authentication-failure both**
event ring-topology-change [Systemlog|SMTP|Both]	**G**	Set X-ring topology changed event type	switch(config)**#event ring-topology-change both**
event systemlog [Link-UP|Link-Down|Both]	**I**	Set port event for system log	switch(config)**#interface fastethernet 3** switch(config-if)**#event systemlog both**

event smtp [Link-UP|Link-Down|Both]	**I**	Set port event for SMTP	switch(config)**#interface fastethernet 3** switch(config-if)**#event smtp both**
show event	**P**	Show event selection	switch**#show event**
no event device-cold-start	**G**	Disable cold start event type	switch(config)**#no event device-cold-start**
no event device-warm-start	**G**	Disable warm start event type	switch(config)**#no event device-warm-start**
no event authentication-failure	**G**	Disable Authentication failure event typ	switch(config)**#no event authentication-failure**
no event X-ring-topology-change	**G**	Disable X-ring topology changed event type	switch(config)**#no event X-ring-topology-change**
no event systemlog	**I**	Disable port event for system log	switch(config)**#interface fastethernet 3** switch(config-if)**#no event systemlog**
no event smpt	**I**	Disable port event for SMTP	switch(config)**#interface fastethernet 3** switch(config-if)**#no event smtp**

SNTP Commands Set

Netstar Commands	Level	Description	Example
sntp enable	**G**	Enable SNTP function	switch(config)#**sntp enable**
sntp daylight	**G**	Enable daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#**sntp daylight**
sntp daylight-period [Start time] [End time]	**G**	Set period of daylight saving time, if SNTP function is inactive, this command can't be applied. Parameter format: [yyyymmdd-hh:mm]	switch(config)# **sntp daylight-period 20060101-01:01 20060202-01:01**
sntp daylight-offset [Minute]	**G**	Set offset of daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#**sntp daylight-offset 3**
sntp ip [IP]	**G**	Set SNTP server IP, if SNTP function is inactive, this command can't be applied.	switch(config)#**sntp ip 192.169.1.1**
sntp timezone [Timezone]	**G**	Set timezone index, use "show sntp timzezone" command to get more information of index number	switch(config)#**sntp timezone 22**

show sntp	**P**	Show SNTP information	switch**#show sntp**
show sntp timezone	**P**	Show index number of time zone list	switch**#show sntp timezone**
no sntp	**G**	Disable SNTP function	switch(config)**#no sntp**
no sntp daylight	**G**	Disable daylight saving time	switch(config)**#no sntp daylight**

X-ring Commands Set

Netstar Commands	Level	Description	Example
ring enable	**G**	Enable X-ring	switch(config)#**ring enable**
ring master	**G**	Enable ring master	switch(config)# **ring master**
ring couplering	**G**	Enable couple ring	switch(config)#**ring couplering**
ring dualhoming	**G**	Enable dual homing	switch(config)#**ring dualhoming**
ring ringport **[1st Ring Port] [2nd Ring Port]**	**G**	Configure 1st/2nd Ring Port	switch(config)#**ring ringport 7 8**
ring couplingport **[Coupling Port]**	**G**	Configure Coupling Port	switch(config)#**ring couplingport 1**
ring controlport **[Control Port]**	**G**	Configure Control Port	switch(config)#**ring controlport 2**
ring homingport **[Dual Homing Port]**	**G**	Configure Dual Homing Port	switch(config)#**ring homingport 3**
show ring	**P**	Show the information of X - Ring	switch#**show ring**
no ring	**G**	Disable X-ring	switch(config)#**no ring**
no ring master	**G**	Disable ring master	switch(config)# **no ring master**
no ring couplering	**G**	Disable couple ring	switch(config)# **no ring couplering**
no ring dualhoming	**G**	Disable dual homing	switch(config)# **no ring dualhoming**

ComNet Customer Service

Customer Care is ComNet Technology's global service center, where our professional staff are ready to answer your questions at any time. Email address of ComNet Global Service Center: customercare@ComNet.net

Communication Networks

World Headquarters
3 Corporate Drive
Danbury, CT 06810 USA
T 203 796-5300
F 203 796-5303
888 678-9427 Tech Support
info@ComNet.net

ComNet Europe Ltd
8 Turnberry Park Road
Gildersome, Morley
Leeds, LS27 7LE, UK
T +44 (0)113 307 6400
F +44 (0)113 253 7462
info-europe@ComNet.net

© 2010 Communication Networks. All rights reserved.

The COMNET logo is a registered trademark of Communication Networks Corporation. Additional Company and product names may be trademarks or registered trademarks of the individual companies and are respectfully acknowledged and do not imply endorsement.